UnderDefense
CYBERSECURITY

Internal penetration testing report

[Anonymized]

Please be informed that this is an incomplete version of the UnderDefense Internal Penetration Testing Report

Get full report

Table of contents

Executive Summary

This report presents the results of the “Gray Box” penetration testing for the [CLIENT_NAME] internal network perimeter. The recommendations provided in this report are structured to facilitate remediation of the identified security risks. This document serves as a formal letter of attestation for the recent [CLIENT_NAME] “Gray Box” internal network penetration testing.
Evaluation ratings compare information gathered during the engagement to “best in class” criteria for security standards. We believe that the statements made in this document provide an accurate assessment of the [CLIENT_NAME]’s current security.
We highly recommend reviewing the Summary section of business risks and High-Level Recommendations for a better understanding of risks and discovered security issues.

Scope of assessment	Security Level	Grade
Internal Network Perimeter	F	Unacceptable
Wireless Network Perimeter	A	Excellent

Grade	Security	Criteria Description
A	Excellent	The security exceeds “Industry Best Practice” standards. The overall posture was found to be excellent with only a few low-risk findings identified.
B	Good	The security meets accepted standards for “Industry Best Practice.” The overall posture was found to be strong with only a handful of medium- and low-risk shortcomings identified.
B	Fair	Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to “Industry Best Practice” standards
D	Poor	Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address exposures identified. Major changes are required to elevate to “Industry Best Practice” standards.
F	Unacceptable	Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources.

1.1 Project Objectives

Our primary goal within this project was to provide the [CLIENT_NAME] with an understanding of the current level of security in the internal network and its infrastructure components. We completed the following objectives to accomplish this goal:

- Identify risks that organizations could be victim of ransomware attack
  - **Confirmed:** Critical severity risk caused by multiple outdated vulnerable business-critical IT systems
- Identifying network-based threats to and vulnerabilities in the Active Directory
  - **Confirmed:** Critical security controls are not in place to meet best practices and protect organizations from instant malware attacks.
- Check for Cyber hygiene
  - **Confirmed:** Critical security controls such as Regular Software Patching & Updates, Strong Password Management, Regular Security Monitoring & Auditing, Network Segmentation based on Zero Trust principals
- Comparing [CLIENT_NAME] current security measures with industry best practices
  - **Does not meet:**
    - Regular Patching and Updates: Ensure that all software, including operating systems, applications, and security tools, are regularly patched and updated with the latest security patches and updates to address known vulnerabilities and weaknesses.
    - Strong Authentication and Access Controls: Enforce the use of strong, unique passwords for all user accounts, implement multi-factor authentication (MFA) wherever possible, and restrict user access permissions based on the principle of least privilege to limit potential exposure to unauthorized access.
    - Incident Response Plan: Develop and maintain an incident response plan that outlines roles and responsibilities, communication protocols, and steps to mitigate and recover from security incidents. Regularly review and update the plan to reflect changes in the threat landscape and organizational environment.
    - Threat Hunt & Threat Intelligence Monitoring: Implement continuous monitoring of corporate data, domains and user's to detect and respond to potential security incidents, such as fraudulent activities, data breaches and leakage, or compromised user's data such as emails, passwords, etc.
  - **Partially meet:**
    - Secure Network Architecture: Implement a secure network architecture that includes network segmentation, firewalls, and intrusion detection/prevention systems (IDPS) to isolate critical systems and data from potential threats and control access to sensitive information.
    - Compliance with Industry Standards: Ensure compliance with relevant industry standards, regulations, and frameworks, such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology

(NIST) Cybersecurity Framework, and others applicable to the art materials and related products industry.

- **Meets best practices:**
  - Backup and Disaster Recovery: Regularly back up critical data and establish a robust disaster recovery plan to ensure that data can be restored in the event of a cybersecurity incident or data loss.
  - Secure Remote Access: Implement secure remote access mechanisms, such as virtual private networks (VPNs) or secure remote desktop protocols, with strong authentication and access controls to protect against unauthorized access to the organization's networks and systems.
- Providing recommendations that [CLIENT_NAME] can implement to mitigate threats and vulnerabilities and meet industry best practices
- Completed: recommendations were provided in section **“1.5 High-Level Recommendations”**

1.2 Scope, Timeframe and Limitations

Testing and verification were performed between [DATE]. The scope of this project was limited to the [CLIENT_NAME] internal network.

We conducted the tests using a production version of the [CLIENT_NAME] internal network. All other servers were out of scope. All testing and verification were conducted from outside of [CLIENT_NAME] offices.

User Accounts provided by [CLIENT_NAME]
The following hosts were considered to be in scope for testing.

Scope	Description
Internal Network Scope	[NETWORK_SCOPE]
Network Devices Scope	[NETWORK_DEVICES_SCOPE]
WiFi Testing Scope	[WIFI_SCOPE]

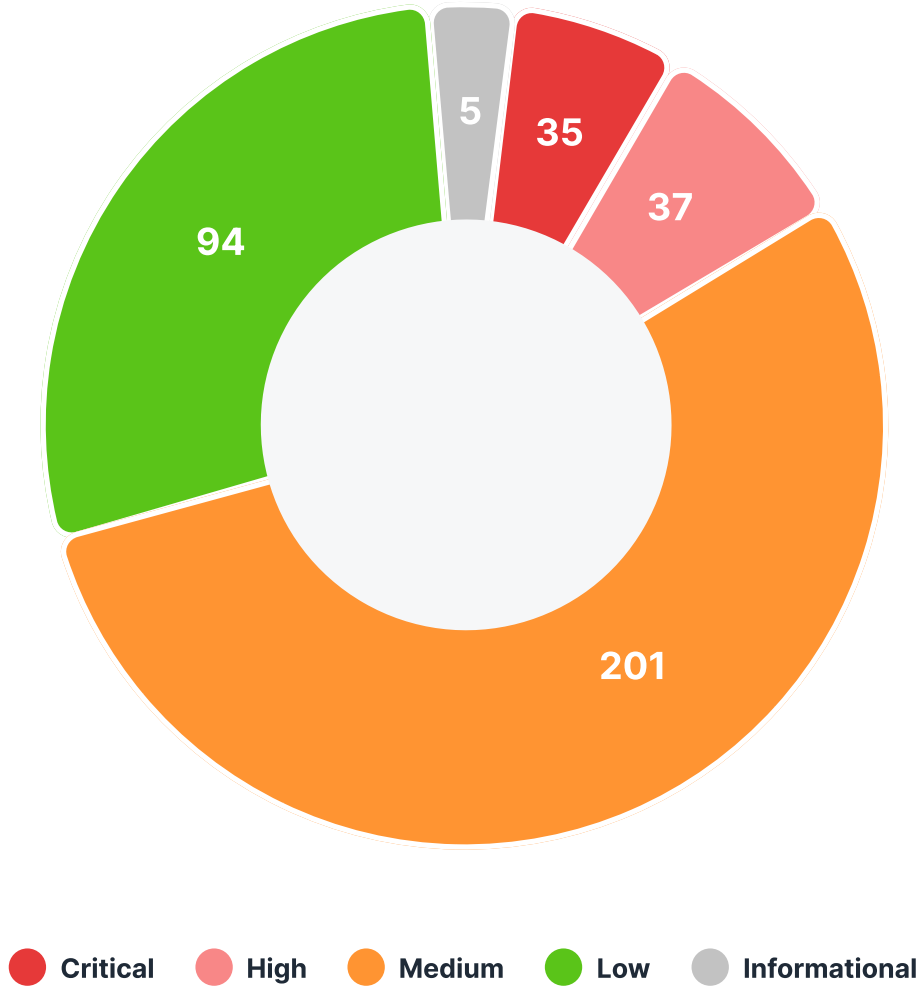
Limitations

This security assessment was conducted for [CLIENT_NAME] production environment and valid on the date of the report submission hereto. The description of findings, recommendations, and risks was valid on the date of submission the report hereto. Any projection to the future of the report’s information is subject to risk due to changes in the Infrastructure architecture, and it may no longer reflect its logic and controls.

1.3 Summary of Findings

Our assessment of the [CLIENT_NAME] internal network revealed the following vulnerabilities:

Vulnerabilities by severity



Security experts performed security testing, which demonstrates the following results

Severity	Critical	High	Medium	Low	Informational
Number of issues by types	35	37	201	94	5

Severity scoring:

- **Critical** – Immediate threat to key business processes
- **High** – Direct threat to key business processes.
- **Medium** – Indirect threat to key business processes or partial threat to business processes.
- **Low** – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
- **Informational** – This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run

The exploitation of found vulnerabilities may cause full compromise of some services, stealing users' accounts, and gaining organizations' and users' sensitive information.

1.4 Summary of Business Risks

Security controls	Business Risks			
	Operational Disruption	Regulatory Compliance	Damage to Reputation	End User Data Disruption
Insecure Network Architecture	Direct impact	Direct impact	Direct impact	Direct impact
Lack of Patching and Software Updates	Direct impact	High risk	High risk	Direct impact
Lack of Security Monitoring	35	Direct impact	Direct impact	Direct impact
Human Related Risks	High risk	High risk	High risk	Direct impact

Financial Loss: If a business's cybersecurity is breached, it can result in financial losses due to theft, fraud, or the cost of remedying the issue. This can include direct costs such as fines, legal fees, and compensation, as well as indirect costs such as reputational damage, loss of customer trust, and loss of revenue.

Operational Disruption: If a business's systems are compromised, it can disrupt their operations, leading to downtime, loss of productivity, and inability to provide services to customers. This can also result in reputational damage, as customers may become frustrated with the lack of service. Based on $750M of company's revenue in 2022 business interruption possesses the risk of $2,054,794 direct losses per day, or 85K per hour (within 24h frame).

Regulatory Compliance: Depending on the industry, businesses may be subject to various regulatory requirements related to cybersecurity. If they fail to comply with these requirements, they may face penalties or fines. Average **GDPR fine for a company in 2022 is $1,758,382 in Europe.**

Data Breaches: A cybersecurity vulnerability can lead to data breaches, which can result in sensitive information being exposed or stolen. This can include personal information of customers or employees, financial information, trade secrets, and other confidential information. Data breaches can result in significant legal and financial consequences, as well as reputational damage. From 2.5% to 5% of world's trade is counterfeit products, resulting in **possible $18,790,00 revenue losses in case of intellectual property theft.**

Damage to Reputation: A cybersecurity breach can damage a business's reputation, especially if sensitive information is exposed. Customers may lose trust in the business, which can result in a loss of revenue and difficulty in acquiring new customers. **According to IBM's Cost of a Data Breach 2022 report, a single data breach on a company cost an average of $9,440,000 in the U.S. in 2022**

Critical

severity issues can lead to severe financial losses caused by operational disruption, data breach involving personal and financial information and / or regulatory compliance:

- Disruption or stoppage of business operations, especially considering that critical systems and data are compromised. This can lead to decreased productivity, revenue loss, and reputational damage. Based on $751.6M of company's revenue in 2022 business interruption possess the **risk of $20M direct losses per day**
- Unauthorized access to sensitive data, including personal (PII) and financial information. Compromise of customers' systems and leakage of sensitive customer data can result in the loss of customer trust and financial loss. Average **GDPR fine for a company in 2022 is $1,758,382 in Europe.** The Industry and Commerce sector lead the list by total number of fines - 369 companies were charged.
- Legal liability for damages resulting from a successful attack, such as financial losses suffered by customers or partners.
- Theft of intellectual property such as trade secrets or proprietary information. This can lead to a loss of competitive advantage and damage to the business's reputation. 2.5% to 5% of world's trade is counterfeit products, resulting in **possible $18,790,00 revenue losses in case of intellectual property theft.**

High

severity issues can lead to full or partial operational disruption. If a business's systems are compromised, it can disrupt their operations, leading to downtime, loss of productivity, and inability to provide services to customers. This can also result in reputational damage, as customers may become frustrated with the lack of service:

- Persisting in the internal network for a long time because of using domain accounts without password expiration. This means malicious actors can stay in your network as long as they need to and wait for the best time to strike.

- Brute forcing users' passwords. Gaining the access to user's session literally breaking them using various automated tools.
- Outdated software versions often have a large number of CVEs and associated exploits, which can result in numerous vulnerabilities. These vulnerabilities can pose significant security risks, potentially leading to unauthorized access to sensitive information, data breaches, and reputational damage for the business.
  60% of cybersecurity breaches happen due to unpatched vulnerabilities.

Medium

severity issues can lead to reputational damages. A cybersecurity breach can damage a business's reputation, especially if sensitive information is exposed. Customers may lose trust in the business, which can result in a loss of revenue and difficulty in acquiring new customers:

- Unauthorized access to different resources can potentially cause sensitive data exposures and reputational losses because of the leakage of documents that belong to certain employees and [CLIENT_NAME] clients.
- Based on current security controls implemented, malicious actors are able to gain a large amount of information about the SNMP server and the network it monitors. This helps to prepare and plan successful attacks. **An average period of time malicious actors stay undetected in the companies network is 280.**
- Obtaining credentials or other sensitive information and to modify traffic exchanged between a client and server.

Low

and informational severity issues can lead to:

- Provide additional internal information that can be used by threat actors for successful attacks on a platform such as a Remote Command Execution, Denial of Service, Directory Traversal etc.
- Theft of database accesses leading to unauthorized access to sensitive data, such as user credentials and transaction records. This can result in reputational damage, loss of customer trust, and legal and regulatory implications.
- Could be chained with other vulnerabilities to increase impact.