HACKTHEBOX

# Wi-Fi Security Assessment

## Report of Findings

**HTB Certified Wi-Fi Pentesting Expert (HTB CWPE) Exam Report**

**Candidate Name: TODO Candidate Name**

**Paxora Pharmaceuticals LLC**

**January 30, 2026**

**Version: 1.0**

# Table of Contents

# 1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

# 2 Engagement Contacts

| Paxora Pharmaceuticals Contacts | | |
|---|---|---|
| **Contact** | **Title** | **Contact Email** |
| Evelyn Hartman | Chief Executive Officer | evelyn@paxora.local |
| Marcus Keegan | Chief Technical Officer | marcus@paxora.local |

| Assessor Contact | | |
|---|---|---|
| **Assessor Name** | **Title** | **Assessor Contact Email** |
| TODO Candidate Name | TODO Candidate Title | TODO Candidate Email |

# 3 Executive Summary

Paxora Pharmaceuticals LLC (“Paxora Pharmaceuticals” herein) contracted TODO Candidate Name to perform a Wi-Fi Security Assessment of Paxora Pharmaceuticals’s environment to identify security weaknesses, determine impact on Paxora Pharmaceuticals’s critical infrastructure, document all findings in a clear and repeatable manner, and provide remediation recommendations.

## 3.1 Approach

TODO Candidate Name performed testing under a “Grey Box” approach from January 29, 2026, to January 30, 2026 with no credentials and minimal advance knowledge of Paxora Pharmaceuticals’ Wi-Fi environment. The goal was to evaluate the security posture of their wireless infrastructure, identify misconfigurations, vulnerabilities, and attack paths, and determine their potential impact. Testing was performed remotely via SSH/RDP from the designated attack hosts at each office, focusing on the in-scope SSIDs and associated internal hosts. Each identified weakness was documented and manually analyzed to determine exploitation possibilities, privilege escalation potential, and lateral movement opportunities. TODO Candidate Name sought to demonstrate the full impact of each vulnerability, up to and including a company-wide compromise. If TODO Candidate Name sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If TODO Candidate Name gained a foothold in the environment, Paxora Pharmaceuticals authorized additional testing to include lateral movement, horizontal/vertical privilege escalation, and validation of implemented security controls, such as antivirus solutions and infrastructure updates, to demonstrate the potential consequences of a complete compromise.

## 3.2 Scope

The scope of this assessment included the internal network ranges for Paxora Pharmaceuticals’ offices, the paxora.local Wi-Fi networks, and any additional Wi-Fi networks owned by Paxora Pharmaceuticals that were discovered during the engagement. Internal access was provided by the client, and a Linux SSH server was installed on their internal network to facilitate the assessment.

### In Scope Assets

| Host/URL/IP Address | Description |
|---|---|
| TODO 10.16.X.X | TODO |
| 172.16.219.9 | Paxora Pharmaceuticals’ Domain controller, internal AD host |
| 172.16.219.0/24 | Paxora Pharmaceuticals’ internal network |
| TODO other discovered internal domain(s) | TODO |

## 3.3 Assessment Overview and Recommendations

During the Wi-Fi Security Assessment of Paxora Pharmaceuticals, TODO Candidate Name identified 2 findings that threaten the confidentiality, integrity, and availability of Paxora Pharmaceuticals' information systems. The findings were categorized by severity level, with TODO 0 of the findings being a high-risk rating, 1 medium-risk, and 0 low risk. There was also 0 informational finding related to improving security monitoring capabilities within the internal network.

TODO EXECUTIVE SUMMARY HERE

Paxora Pharmaceuticals should create a remediation plan based on the Remediation Summary section of this report, addressing all high-risk findings as soon as possible according to the needs of the business. Given the comprehensive nature of this in-depth Wi-Fi security assessment test, Paxora Pharmaceuticals should focus on implementing the recommendations provided to address misconfigurations, privilege escalation paths, and lateral movement opportunities.

To maintain a robust security posture, Paxora Pharmaceuticals should also consider scheduling periodic Wi-Fi security assessments and penetration tests to validate improvements and identify emerging vulnerabilities. Continuous monitoring and proactive hardening of the Wi-Fi environment will make it increasingly challenging for attackers to compromise the network and will improve Paxora Pharmaceuticals' ability to detect and respond to suspicious activity effectively.

# 4 Wi-Fi Penetration Test Assessment Summary

TODO Candidate Name began all testing activities from the perspective of an unauthenticated user on the internal network of Paxora Pharmaceuticals. Paxora Pharmaceuticals provided the tester with internal network access via the Linux SSH server, but did not provide additional information such as configuration details.

## 4.1 Summary of Findings

During the course of testing, TODO Candidate Name uncovered a total of 2 findings that pose a material risk to Paxora Pharmaceuticals' information systems. As requested by Paxora Pharmaceuticals, this assessment focuses exclusively on findings with medium and high impact, ensuring that all documented vulnerabilities and recommendations are directly relevant to risks that could significantly affect the confidentiality, integrity, and availability of Paxora Pharmaceuticals' systems. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 Critical** and **1 Medium** vulnerabilities were identified:

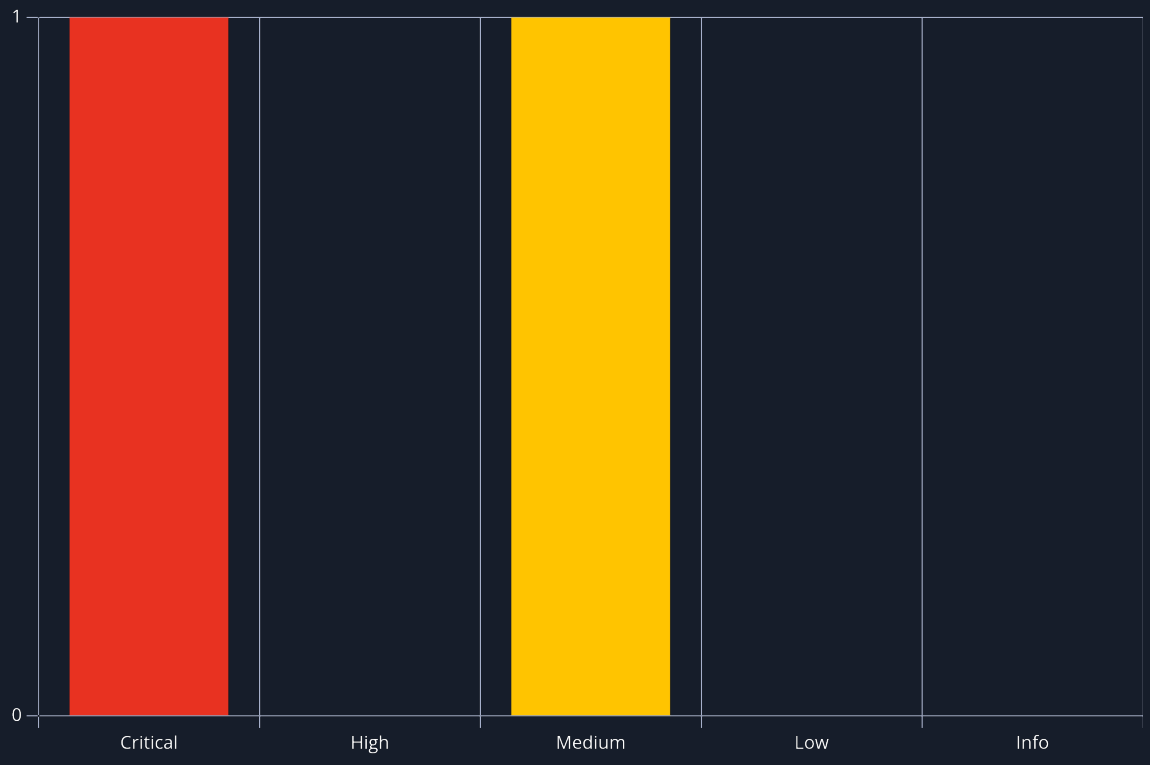


**Figure 1 - Distribution of identified vulnerabilities**

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

| # | Severity Level | Finding Name | Page |
|---|---|---|---|
| 1 | 9.9 (Critical) | LLMNR/NBT-NS Response Spoofing | 10 |
| 2 | 6.4 (Medium) | Insecure File Shares | 12 |

# 5 Internal Network Compromise Walkthrough

During the course of the assessment TODO Candidate Name was able to gain a foothold within the internal network via the provided access through the Linux SSH server, move laterally, and compromise the internal network, leading to full administrative control over the `paxora` wi-fi network and TODO INSERT NETWORK NAME Wi-Fi network.

The steps below outline the actions taken from initial access to compromise. This attack chain does not encompass all vulnerabilities and misconfigurations discovered during the assessment. Any issues not directly used as part of the attack chain are documented separately in the Technical Findings Details section, ranked by severity level.

The purpose of this attack chain is to demonstrate to Paxora Pharmaceuticals the potential impact of the vulnerabilities identified in this report and how they interconnect to represent the overall risk to the environment. This approach also helps to prioritize remediation efforts - patching even two critical flaws could disrupt the attack chain significantly while allowing the organization time to address other reported issues.

Although additional findings detailed in this report could potentially lead to a similar level of access, this documented attack chain represents the path of least resistance taken by the assessor to achieve domain compromise.

## 5.1 Detailed Walkthrough

TODO Candidate Name performed the following to fully compromise the `paxora` wi-fi networks.

1. TODO LIST HIGH LEVEL STEPS
2. ...

**Detailed reproduction steps for this attack chain are as follows:** TODO FILL IN DETAILED ATTACK CHAIN STEPS

TODO Candidate Namethen performed the following to fully compromise the TODO INSERT OTHER NETWORK NAME(S) network.

1. TODO LIST HIGH LEVEL STEPS
2. ...

**Detailed reproduction steps for this attack chain are as follows:** TODO FILL IN DETAILED ATTACK CHAIN STEPS

# 6 Remediation Summary

As a result of this assessment there are several opportunities for Paxora Pharmaceuticals to strengthen its internal network and Wi-Fi security. Remediation efforts are prioritized below, starting with those that will likely take the least amount of time and effort to complete. Paxora Pharmaceuticals should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

## 6.1 Short Term

TODO SHORT TERM REMEDIATION:

- Finding Reference 1 - Example remediation

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

## 6.2 Medium Term

TODO MEDIUM TERM REMEDIATION:

- Finding Reference 1 - Example remediation
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

## 6.3 Long Term

TODO LONG TERM REMEDIATION:

- TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

# 7 Technical Findings Details

## 1. LLMNR/NBT-NS Response Spoofing - Critical

| | |
|---|---|
| CWE | CWE-522 - Insufficiently Protected Credentials |
| CVSS 3.1 | 9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |
| Root Cause | By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary-controlled system. This activity may be used to collect or relay authentication materials. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. |
| Impact | Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary-controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary-controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through Network Sniffing and crack the hashes offline through Brute Force to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary-controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system relay step can happen in conjunction with poisoning but may also be independent of it.<br><br>Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and Responder. |
| Affected Component | PAXORA.LOCAL |
| Remediation | • Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment<br>• Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB<br>• Signing can stop NTLMv2 relay attacks.<br>• Network intrusion detection and prevention systems that can identify traffic patterns indicative of MiTM activity can be used to mitigate activity at the network level. |

| | |
|---|---|
| | • Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of MiTM activity. |
| References | https://attack.mitre.org/techniques/T1557/001/ |

## Finding Evidence

TODO DETAILED REPRODUCTION STEPS

Running the Responder tool to attempt to obtain user account password hashes.

Successfully cracking a password hash with Hashcat to reveal the clear text password value.

## 2. Insecure File Shares - Medium

| | |
|---|---|
| CWE | CWE-284 - Improper Access Control |
| CVSS 3.1 | 6.4 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |
| Root Cause | The tester uncovered multiple file shares where all Domain Users have read/write access. |
| Impact | An attacker who gains a foothold in this domain can use this access to search for files containing sensitive data such as credentials and potentially write malicious files to the file shares. |
| Affected Component | PAXORA.LOCAL |
| Remediation | Review file share privileges to ensure that users are granted access in accordance with the principal of least privilege. |
| References | https://attack.mitre.org/techniques/T1135/ |

### Finding Evidence

Viewing file shares accessible to a standard Domain user with the CrackMapExec tool.

# A Appendix

## A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Paxora Pharmaceuticals' data.

| Rating | CVSS Score Range |
|---|---|
| Critical | 9.0 – 10.0 |
| High | 7.0 – 8.9 |
| Medium | 4.0 – 6.9 |
| Low | 0.1 – 3.9 |
| Info | 0.0 |

## A.2 Wi-Fi Networks & Hosts Discovery

| IP Address | Port | Service | Notes |
|---|---|---|---|
| TODO FILL IN AS APPROPRIATE | | | |

## A.3 Subdomain Discovery

| URL | Description | Discovery Method |
|---|---|---|
| TODO FILL IN DISCOVERED VHOSTS/SUBDOMAINS | | |

## A.4 Exploited Hosts

| Host | Scope | Method | Notes |
|---|---|---|---|
| TODO FILL IN AS APPROPRIATE | Text | Text | Text |

## A.5 Compromised Users

| Username | Type | Method | Notes |
|---|---|---|---|
| TODO FILL IN AS APPROPRIATE | Text | Text | Text |

## A.6 Changes/Host Cleanup

| Host | Scope | Change/Cleanup Needed |
|---|---|---|
| TODO FILL IN AS APPROPRIATE | | |

## A.7 Flags Discovered

| Flag # | Host | Flag Value | Flag Location | Method Used |
|---|---|---|---|---|
| 1. | TODO HOSTNAME | TODO MD5 HASH | TODO Administrator's desktop | TODO Exploit CVE-XXX-XXXX (example) |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |
| 7. | | | | |
| 8. | | | | |
| 9. | | | | |
| 10. | | | | |
| 11. | | | | |
| 12. | | | | |
| 13. | | | | |

*End of Report*

*This report was rendered*
*by SysReptor with*
♥