Text, logo

Description automatically generated with medium confidence



Penetration Test Assignment

**Internal Report of Findings**

**Luminex Ltd.**

March 7, 2025

Version 1.0

Table of Contents

[Statement of Confidentiality 3](#__RefHeading___Toc4487_1100251792)

[Engagement Contacts 3](#__RefHeading___Toc4489_1100251792)

[Executive Summary 3](#__RefHeading___Toc4491_1100251792)

[Approach 3](#__RefHeading___Toc4533_1100251792)

[Assignment 4](#__RefHeading___Toc4507_1100251792)

[Objective: 4](#__RefHeading___Toc4505_1100251792)

[Assignment Overview: 4](#__RefHeading___Toc4503_1100251792)

[Scope 4](#__RefHeading___Toc4531_1100251792)

[Reporting and Deliverables 5](#__RefHeading___Toc4457_1119289821)

[Rules of Engagement 5](#__RefHeading___Toc4455_1119289821)

[Network Penetration Test Assessment Summary 6](#__RefHeading___Toc4493_1100251792)

[Summary of Findings 6](#__RefHeading___Toc4527_1100251792)

[Exploited Hosts 7](#__RefHeading___Toc4471_1119289821)

[Compromised Users 7](#__RefHeading___Toc4469_1119289821)

[Changes/Host Cleanup 7](#__RefHeading___Toc4511_1100251792)

[Internal Network Compromise Walkthrough 8](#__RefHeading___Toc4495_1100251792)

[Detailed Walkthrough 8](#__RefHeading___Toc4525_1100251792)

[Collected Evidence 9](#__RefHeading___Toc4499_1100251792_Copy_1)

[Remediation Summary 11](#__RefHeading___Toc4497_1100251792)

[Short Term 11](#__RefHeading___Toc4523_1100251792)

[Medium Term 11](#__RefHeading___Toc4521_1100251792)

[Long Term 11](#__RefHeading___Toc4519_1100251792)

[Appendices 12](#__RefHeading___Toc4501_1100251792)

[Appendix A – Finding Severities 12](#__RefHeading___Toc4517_1100251792)

# 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.

# Engagement Contacts

| **Assessor Contact** | | |
| --- | --- | --- |
| **Assessor Name** | **Title** | **Assessor Contact Email** |
| Hack The Box Academy | Project Director | mgmt@htbacademy.htb |
| Hack The Box Academy | Junior Security Consultant | htb-student@htbacademy.htb |

# Executive Summary

Luminex Ltd. (“Luminex” herein) contracted Hack The Box Academy to perform a Network Penetration Test of Luminex’s internally facing network to identify security weaknesses, determine the impact to Luminex, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

Hack The Box Academy is performing testing under a “black box” approach January 16, 2025, to January 31, 2025 without credentials or any advance knowledge of Luminex’s internally facing environment with the goal of identifying unknown weaknesses. Testing is performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing is performed remotely via a host that was provisioned specifically for this assessment. Each weakness identified is documented and manually investigated to determine exploitation possibilities and escalation potential. Hack The Box Academy seek to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Hack The Box Academy is able to gain a foothold in the internal network, Luminex allows for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

# Assignment

From: Project Director To: <student’s name> (Tester)

Start: <start date> End: <end date>

Objective:

Conduct a penetration test of the assigned network segment and assist the penetration testing team to identify and document all vulnerabilities, assess potential risks, and provide actionable remediation steps.

Assignment Overview:

You have been assigned to perform a penetration test on a specific segment of Luminex organization’s network. This test will focus on uncovering vulnerabilities in the infrastructure, services, configurations of the network, and assist your team.

Scope

The scope of this assessment is one internal network segment consisting of five hosts and the luminex.htb domain.

In-Scope Assets

| **Host/URL/IP Address** | **Description** |
| --- | --- |
| 192.168.195.10/32 | Luminex Web Server |
| 192.168.195.20/32 | Luminex Software Development Server |

Table 1: Scope Details

Reporting and Deliverables

* Detailed report documenting identified vulnerabilities and technical details including step-by-step walkthrough for each penetration testing stage and screenshots.
* Risk ratings (High, Medium, Low) based on the Common Vulnerability Scoring System (CVSS).
* Proof-of-Concept (PoC) for exploited vulnerabilities (where applicable).
* Recommended remediation steps for each vulnerability.

Rules of Engagement

* No testing outside the defined scope.
* Obtain permission before attempting exploitation of vulnerabilities.
* Maintain documentation of all activities and findings.
* Avoid disruption of services or downtime unless explicitly authorized.
* DoS (denial-of-service) or other potentially service-impacting tests are prohibited.

# Network Penetration Test Assessment Summary

Tester began all testing activities from the perspective of an unauthenticated user on the internal network. Project Director provided the tester with network ranges but did not provide any additional information.

Summary of Findings

During the course of testing, the Tester uncovered a total of seven (7) findings that pose a material risk to Luminex’s information systems. The Tester also identified one informational finding that, if addressed, could further strengthen Luminex’s overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

| **Finding Severity** | | | |
| --- | --- | --- | --- |
| **High** | **Medium** | **Low** | **Total** |
| **3** | **1** | **1** | **5** |

Table 2: Severity Summary

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

| **Finding #** | **Severity Level** | **Finding Name** |
| --- | --- | --- |
| 1. | **High** | Exposed and Unprotected SSH Private Key |
| 2. | **High** | Exposed History File with Credentials |
| 3. | **High** | Vulnerable WordPress Plugin with RCE |
| 4. | **Medium** | Anonymous FTP Access |
| 5. | **Low** | Directory Listing in FTP Enabled |

Table 3: Finding List

Exploited Hosts

| **Host** | **Scope** | **Method** | **Notes** |
| --- | --- | --- | --- |
| 192.168.195.204 (Ubuntu) | Internal | Sudo Privilege Abuse | Nano Shell Escape |
| 192.168.195.205 (WIN01) | Internal | Schedule Task Abuse | Code Injection |

Table 4: Exploitation Attempt Details

Compromised Users

| **Username** | **Host** | **Method** | **Notes** |
| --- | --- | --- | --- |
| **john** | 192.168.195.10 | SSH Private Key & Leaked Credentials | Sudo User |
| **www-data** | 192.168.195.10 | WordPress Hash Form Plugin RCE | Web Server User |
| **john** | 192.168.195.20 | Credentials Reuse | Standard User |

Table 5: User Accounts Compromised

Changes/Host Cleanup

| **Host** | **Scope** | **Change/Cleanup needed** |
| --- | --- | --- |
| 192.168.195.10 (Ubuntu) | Internal | Linpeas.sh file in /home/john | linpeas.sh | md5sum: db7d6def7d80b8e982f3359875ea54e3 |
| 192.168.195.20 (WIN01) | Internal | Winpill file in C:\winpill.ps1 | winpill.ps1 | md5sum: 5391c4a8af1ede757ba9d28865e75853 |

Table 6: Assessment Artifacts

# Internal Network Compromise Walkthrough

During the course of the assessment the Tester was able gain a foothold and compromise the internal network, leading to full administrative control over the Luminex.htb network segment. The steps below demonstrate the steps taken from initial access to compromise. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Detailed Walkthrough section, ranked by severity level. The intent of this attack chain is to demonstrate to Luminex the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

Detailed Walkthrough

The Tester performed the following steps to fully compromise the Luminex.htb network segment.

| **Step #** | **Target** | **Action/Command** | **Result** |
| --- | --- | --- | --- |
| 1.1 | **192.168.195.10** | nmap -sV –open -p- 192.168.195.10 | Open ports: 21, 22, 80, 443, 8000 |
| 1.2 | **192.168.195.10** | ftp 192.168.195.10 -P 21 # anonymous:anon | Anonymous login available |
| 1.x | **192.168.195.10** | … | ... |
| 2.1 | **192.168.195.20** | nmap -sV –open -p- 192.168.195.20 | Open ports: 22, 135, 139, 445, 3000, 3389 |
| 2.x | **192.168.195.20** | … | ... |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 7: Exploitation Steps

Collected Evidence

**1.1 – 192.168.195.10 – Port & Service Discovery**

|  |
| --- |
| $ sudo nmap -p- -sV 10.129.12.10 -T5 --open   Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 14:55 EST  Nmap scan report for cube-case.htb (10.129.12.10)  Host is up (0.048s latency).  Not shown: 65527 closed tcp ports (reset)  PORT STATE SERVICE VERSION  21/tcp open ftp ProFTPD  22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)  80/tcp open http nginx 1.18.0 (Ubuntu)  443/tcp open ssl/http Apache httpd 2.4.52 ((Ubuntu))  8000/tcp open ssl/http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)  8001/tcp open ssl/vcom-tunnel?  8080/tcp open http Apache httpd 2.4.52 ((Ubuntu))  8889/tcp open ssl/http Golang net/http server  Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  Nmap done: 1 IP address (1 host up) scanned in 61.99 seconds |

**Finding 1: Port & Service Discovery**

**1.2 – 192.168.195.10 – FTP Anonymous Access on port 21/tcp**

|  |
| --- |
| $ ftp 10.129.12.10 21  Connected to 10.129.12.10.  220 ProFTPD Server (Debian) [10.129.12.10]  Name (10.129.12.10:pwnbox): anonymous   331 Anonymous login ok, send your complete email address as your password  Password: anonymous   230 Anonymous access granted, restrictions apply Remote system type is UNIX.  Using binary mode to transfer files. |

**Finding 2: FTP Anonymous Access**

|  |
| --- |
| ftp> ls -al  229 Entering Extended Passive Mode (|||42851|)  150 Opening ASCII mode data connection for file list  drwxr-x--- 4 john john 4096 Feb 16 17:28 .  drwxr-x--- 4 john john 4096 Feb 16 17:28 ..  -rw------- 1 john john 1153 Feb 15 21:13 .bash\_history  -rw-r--r-- 1 john john 220 Jan 6 2022 .bash\_logout  -rw-r--r-- 1 john john 3771 Jan 6 2022 .bashrc  drwx------ 2 john john 4096 Feb 15 17:16 .cache  -rw------- 1 john john 20 Feb 16 16:34 .lesshst  -rw-r--r-- 1 john john 807 Jan 6 2022 .profile  drwxrwxr-x 2 john john 4096 Feb 12 13:55 .ssh  -rw-r--r-- 1 john john 0 Feb 11 10:18 .sudo\_as\_admin\_successful  -rw------- 1 john john 17094 Feb 15 22:14 .viminfo  -rw-rw-r-- 1 john john 964 Feb 15 22:14 WordPress\_Blog\_Setup\_Update.txt  226 Transfer complete  ftp> get WordPress\_Blog\_Setup\_Update.txt  local: WordPress\_Blog\_Setup\_Update.txt remote: WordPress\_Blog\_Setup\_Update.txt  229 Entering Extended Passive Mode (|||12725|)  150 Opening BINARY mode data connection for WordPress\_Blog\_Setup\_Update.txt (964 bytes)  100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 964 14.97 KiB/s 00:00 ETA  226 Transfer complete 964 bytes received in 00:00 (7.92 KiB/s)  ftp> get .bash\_history local: bash\_history remote: bash\_history  229 Entering Extended Passive Mode (|||39373|)  150 Opening BINARY mode data connection for bash\_history (1285 bytes)  100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 1285 51.01 KiB/s 00:00 ETA  226 Transfer complete 1285 bytes received in 00:00 (10.95 KiB/s)  ftp> cd .ssh  ftp> ls -al  229 Entering Extended Passive Mode (|||26184|)  150 Opening ASCII mode data connection for file list  -rw------- 1 john john 2602 Feb 12 13:55 id\_rsa  -rw-r--r-- 1 john john 565 Feb 12 13:55 id\_rsa.pub  226 Transfer complete  ftp> get id\_rsa local: id\_rsa remote: id\_rsa 229 Entering Extended Passive Mode (|||41007|)  150 Opening BINARY mode data connection for id\_rsa (2602 bytes)  100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 2602 108.80 KiB/s 00:00 ETA  226 Transfer complete 2602 bytes received in 00:00 (22.28 KiB/s) |

Finding 3: Obtaining Sensitive Files from FTP

# Remediation Summary

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

Short Term

* [**Finding 2**] – Disable Anonymous Access on the FTP server
* [**Finding 3**] – Change the default FTP directory which doesn’t contain sensitive files
* [**Finding 7**] – Update the WordPress Hash Form Plugin to the latest version

Medium Term

* [**Finding 5**] – Enforce Strong Password Policies (12+ characters)
* [**Finding 12**] – Enforce Unique Password Usage

Long Term

* Perform ongoing internal network vulnerability assessments
* Educate systems and network administrators and developers on security hardening best practices compromise

# Appendices

Appendix A – Finding Severities

Each finding has been assigned a severity rating of high, medium, or low. 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 Luminex’s data.

| **Rating** | **Severity Rating Definition** |
| --- | --- |
| **High** | Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited. |
| **Medium** | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR -  The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |
| Low | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR -  The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |

Table 8: Severity Definitions