HACKTHEBOX

Cybersecurity Assessment

CJCA Exam Report

Internal Report of Findings

HTB Junior Cybersecurity Associate (CJCA) Exam Report

Candidate Name: TODO Candidate Name

TODO Customer Ltd.

Version: TODO 1.0

Table of Contents

1 Statement of Confidentiality 4
2 Engagement Contacts 5
3 Executive Summary 6
3.1 Approach 6
4 Assignment 7
4.1 Objective 7
4.2 Assignment Overview 7
5 Phase 1: Grey Box Penetration Test 8
5.1 Scope 8
5.2 Reporting and Deliverables 8
5.3 Rules of Engagement 8
6 Network Penetration Test Assessment Summary 10
6.1 Summary of Findings 10
6.2 Exploited Hosts 11
6.3 Compromised Users 11
6.4 Changes / Host Cleanup 11
7 Internal Network Compromise Walkthrough 12
7.1 Detailed Walkthrough 12
7.2 Collected Evidence 12
8 Remediation Summary 15
8.1 Short Term 15
8.2 Medium Term 15
8.3 Long Term 15
9 Phase 2: SIEM Alert Validation and Analysis 16

9.1 Scope 16
9.2 Deliverables 16
9.3 SIEM Alerts 16
9.4 SIEM Alert Validation and Analysis 16

10 Technical Findings Details 18
Exposed and Unprotected SSH Private Key 18
Exposed History File with Credentials 19
Vulnerable WordPress Plugin with RCE 20
Anonymous FTP Access 21
Directory Listing in FTP Enabled 22

A Appendix 23
A.1 Finding Severities 23
A.2 Flags Discovered 23

1 Statement of Confidentiality

The contents of this document have been developed by TODO Assessor Ltd.. TODO Assessor Ltd. 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 TODO Assessor Ltd.. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of TODO Assessor Ltd..

The contents of this document do not constitute legal advice. TODO Assessor Ltd.'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 TODO Assessor Ltd. external or internal infrastructure.

2 Engagement Contacts

TODO Customer Contacts		
Contact	**Title**	**Contact Email**
Luminex Ltd.	Manager	mgmt@luminex.htb

TODO Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Acme Security, LLC.	Project Director	mgmt@acmesecurity.htb
Acme Security, LLC.	Junior Cybersecurity Analyst	TODO Student Email

3 Executive Summary

TODO Customer Ltd. (“TODO Customer” herein) contracted TODO Candidate Name to perform a Network Penetration Test of TODO Customer’s externally facing network to identify security weaknesses, determine the impact to TODO Customer, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

TODO Assessor Ltd. will conduct the assessment in two sequential phases under controlled conditions to simulate realistic attack scenarios while minimizing disruption.

Phase 1: Grey Box Penetration Test

Testing will be performed under a "grey box" approach, where TODO Assessor Ltd. has limited prior knowledge of TODO Customer’s environment (e.g., basic network diagrams or IP ranges) but no credentials or detailed internal configurations. The objective is to identify unknown weaknesses from an attacker's perspective with partial visibility. Testing will be conducted remotely via a provisioned host, adopting a non-evasive standpoint initially to uncover misconfigurations and vulnerabilities through reconnaissance, scanning, and targeted exploitation. Each identified weakness will be documented and manually investigated for exploitation possibilities, including potential foothold establishment, lateral movement, and horizontal/vertical privilege escalation. If a foothold is gained, TODO Customer authorizes further internal testing to demonstrate the full impact of a compromise, such as data exfiltration or domain control, while adhering to rules of engagement to avoid production impacts.

Phase 2: SIEM Alert Validation and Analysis

Following the penetration test, TODO Customer’s security team will reproduce the identified attack paths in a controlled staging environment. These simulations will generate telemetry data, which will be ingested into their Elastic SIEM platform. Based on this data, the SIEM will generate security alerts tied to the techniques used during the simulated attacks. TODO Assessor Ltd. will review these alerts to determine whether each one represents a true positive or a false positive, providing supporting evidence from the SIEM logs for each decision.

Throughout both phases, TODO Assessor Ltd. will prioritize safety, with predefined escalation protocols for any high-risk findings, and collaborate with TODO Customer's IT/security team for validation and controlled testing.

4 Assignment

- **From:** Project Director
- **To:** TODO Candidate Name (Tester)
- **Start:**
- **End:**

4.1 Objective

Help TODO Customer understand how an attacker could navigate their environment, identify the risks present within the in-scope segment of their network, and evaluate the accuracy and coverage of their detection rules.

4.2 Assignment Overview

You are a Junior Cybersecurity Analyst at TODO Assessor Ltd.. Following a recent surge in suspicious activity and growing concerns about internal threats, TODO Customer Ltd. has engaged your team to perform a comprehensive internal cybersecurity assessment of a certain segment of its corporate network. This engagement includes not only identifying vulnerabilities through targeted attack simulation, but also evaluating the effectiveness of TODO Customer's Security Information and Event Management (SIEM) detections in identifying those threats. Once the assessment is complete, compose and submit a commercial-grade report . The report should include all identified vulnerabilities, step-by-step evidence of successful exploitation, and clear remediation recommendations. When documenting your alert classifications, follow the same step-by-step approach to provide evidence and justification for each decision.

5 Phase 1: Grey Box Penetration Test

5.1 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
NIX01	Luminex Software Development Server
NIX02	Luminex Email Server
WEB01	Luminex Web Server
WIN01	Luminex Windows Client
WIN02	Luminex Windows Management Server
TODO	TODO

5.2 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.

5.3 Rules of Engagement

- Sensitive or personally identifiable information disclosure
- Remote Code Execution (RCE)
- Arbitrary file upload
- Authentication or authorization flaws
- All forms of injection vulnerabilities
- Directory Traversal
- Local File Read
- Significant Security misconfigurations and business logic flaws
- Exposed credentials that could be leveraged to gain further accessed
- Windows and Linux local privilege escalation vulnerabilities
- Vulnerable services and applications

The following types of activities are considered out-of-scope for this penetration test:

- Scanning and assessing any other IP in the entry point's network or hosts that do not fall within the in-scope internal subnets
- Physical attack against TODO Customer properties

- Unverified scanner output
- Any vulnerabilities identified through DDoS or spam attacks
- Self-XSS Login/logout CSRF
- Issues with SSL certificates, open ports, TLS versions, or missing HTTP response headers
- Vulnerabilities in third-party libraries unless they can be leveraged to significantly impact the targeted
- Any theoretical attack or attacks that require significant user interaction or low risk
- Phishing or social engineering attack against TODO Customer employees or contractors

6 Network Penetration Test Assessment Summary

TODO Candidate Name 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.

6.1 Summary of Findings

During the course of testing, TODO Candidate Name uncovered a total of 5 findings that pose a material risk to TODO Customer's information systems. TODO Candidate Name also identified 0 informational finding that, if addressed, could further strengthen TODO Customer'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 chart provides a summary of the findings by severity level.

In the course of this penetration test **3 High**, **1 Medium** and **1 Low** vulnerabilities were identified:

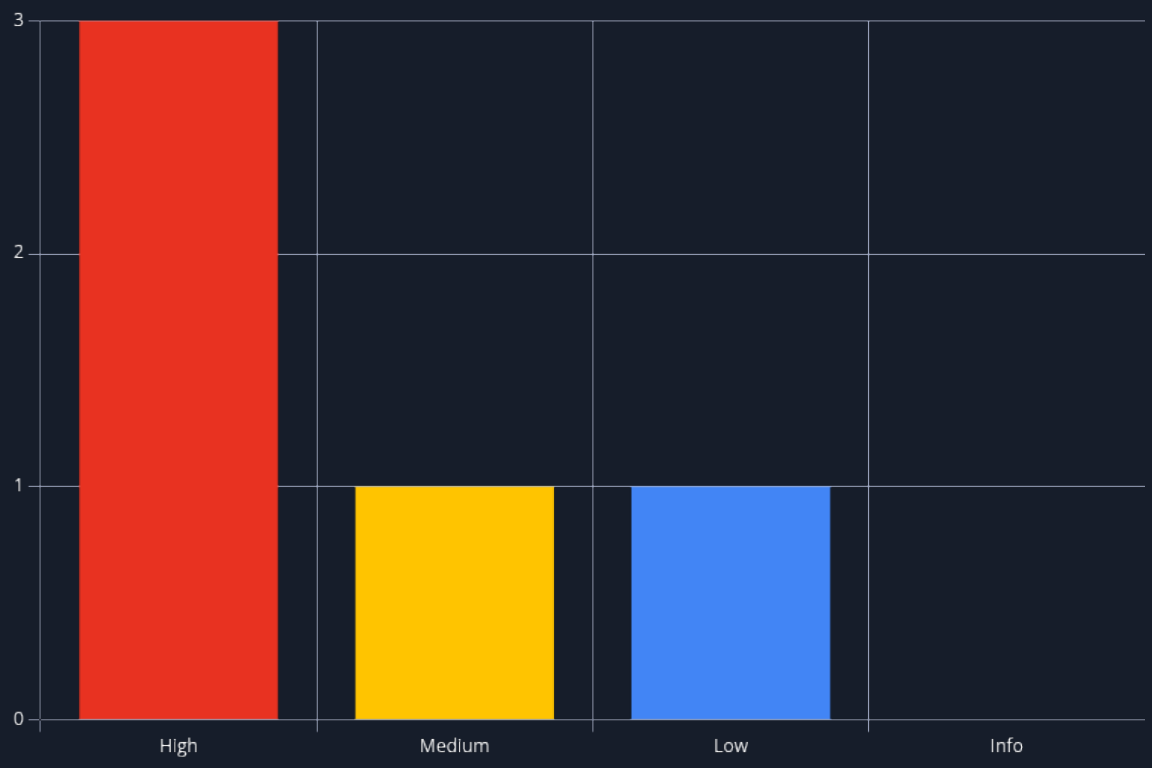

Figure 1 - Distribution of identified vulnerabilities

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	High	Exposed and Unprotected SSH Private Key	18

#	Severity Level	Finding Name	Page
2	High	Exposed History File with Credentials	19
3	High	Vulnerable WordPress Plugin with RCE	20
4	Medium	Anonymous FTP Access	21
5	Low	Directory Listing in FTP Enabled	22

6.2 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
TODO	TODO	TODO	TODO

6.3 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	Credential Reuse	Standard User
TODO	TODO	TODO	TODO

6.4 Changes / Host Cleanup

Host	Scope	Change / Cleanup needed
192.168.195.10 (Ubuntu)	Internal	Linpeas.sh file in /home/john
192.168.195.20 (WIN01)	Internal	Winpill file in C:\winpill.ps1
TODO	TODO	TODO

7 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 TODO INSERT NETWORK SEGMENT NAME 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 TODO Customer 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.

7.1 Detailed Walkthrough

TODO Candidate Nameperformed the following to fully compromise the TODO INSERT NETWORK SEGMENT NAME network segment.

Step #	IP/Host/ 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	…	…
TODO	TODO	TODO	TODO

7.2 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
```

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.
```

```
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 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)
```

8 Remediation Summary

As a result of this assessment there are several opportunities for TODO Customer 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. TODO Customer should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

8.1 Short Term

TODO SHORT TERM REMEDIATION:

- TODO Finding Reference 2 - Disable Anonymous Access on the FTP server
- TODO Finding Reference 3 - Change the default FTP directory which doesn't contain sensitive files
- TODO Finding Reference 7 - Update the WordPress Hash Form Plugin to the latest version
- TODOFinding Reference X - TODO FILL IN AS APPROPRIATE

8.2 Medium Term

TODO MEDIUM TERM REMEDIATION:

- TODO Finding Reference 1 - Disable LLMNR and NBT-NS wherever possible
- TODO Finding Reference 12 - Enforce Unique Password Usage
- TODO Finding Reference 2 - TODO FILL IN AS APPROPRIATE

8.3 Long Term

TODO LONG TERM REMEDIATION:

- Perform ongoing internal network vulnerability assessments
- Educate systems and network administrators and developers on security hardening best practices compromise
- TODO FILL IN AS APPROPRIATE

9 Phase 2: SIEM Alert Validation and Analysis

9.1 Scope

In phase 2, TODO Customer's security team reproduced the attack paths identified during the penetration test in a controlled staging environment. These simulations generated telemetry data, which was ingested into the Elastic SIEM platform, resulting in security alerts based on the techniques used. The generated alerts are documented under SIEM Alerts below.

In-Scope Assets

Host/URL/IP Address	Description
ELK01	Luminex Elastics SIEM
TODO	TODO

9.2 Deliverables

The analyst will review the security alerts generated by TODO Customer's Elastic SIEM platform in response to the simulated attacks executed in the controlled staging environment. These evaluations will be presented in a dedicated table titled "SIEM Alert Validation and Analysis" within the report, classifying each alert as a true positive (confirmed malicious activity or legitimate threat based on log analysis) or a false positive (benign activity erroneously flagged as malicious, such as overly sensitive detection rules, legitimate administrative/operating system activity, etc.). Evidence for each classification will be derived from SIEM log analysis.

9.3 SIEM Alerts

No.	Alert Name	Description	Host	Alert Timestamp
1	[Placeholder]	TODO The actual SIEM alerts can be found in the report template, which can be downloaded form within the HTB CJCA exam lab after starting the exam.	XXX	XXX
2	XXX	XXX	XXX	XXX
3	XXX	XXX	XXX	XXX
4	XXX	XXX	XXX	XXX

9.4 SIEM Alert Validation and Analysis

Alert No.	True Positive	False Positive	Evidence
1	X		TODO Evidence
2	Text	X	TODO Evidence

Alert No.	True Positive	False Positive	Evidence
3			
4			
5			
6			

10 Technical Findings Details

1. Exposed and Unprotected SSH Private Key - Info

CWE	-
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

2. Exposed History File with Credentials - Info

CWE	-
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

3. Vulnerable WordPress Plugin with RCE - Info

CWE	-
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

4. Anonymous FTP Access - Info

CWE	-
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

5. Directory Listing in FTP Enabled - Info

CWE	-
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

A Appendix

A.1 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 TODO Customer'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.

A.2 Flags Discovered

The Tester found the following flags on compromised hosts in the TODO FILL IN NETWORK SEGMENT NAME network segment.

IP/Host/Target	File name	Flag
192.168.195.10	user.txt	[flag]

IP/Host/Target	File name	Flag
192.168.195.10	root.txt	[flag]
192.168.195.20	...	...
192.168.195.20	...	...
192.168.195.30	...	...
TODO	...	...
TODO	...	...
TODO	...	...

End of Report

This report was rendered
by SysReptor with
♥