HACKTHEBOX

Penetration Test

HTB CPTS Demo

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: TODO Candidate Name

TODO Customer Ltd.

Version: TODO 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

TODO Customer Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
TODO Candidate Name	TODO Candidate Title	TODO Candidate 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 Candidate Name performed testing under a “Black Box” approach from , to without credentials or any advance knowledge of TODO Customer’s externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from TODO Candidate Name's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. TODO Candidate Name sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If TODO Candidate Name were able to gain a foothold in the internal network, TODO Customer as a result of external network testing, TODO Customer allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address, two internal network ranges, the TODO INSERT DOMAIN NAME Active Directory domain, and any other Active Directory domains owned by TODO Customer discovered if internal network access were achieved.

In Scope Assets

Host/URL/IP Address	Description
TODO 10.129.X.X	TODO
172.16.139.0/24	TODO Customer internal network
172.16.210.0/24	TODO Customer internal network
TODO	TODO Customer internal AD domain
TODO other discovered internal domain(s)	TODO

3.3 Assessment Overview and Recommendations

During the penetration test against TODO Customer, TODO Candidate Name identified 1 findings that threaten the confidentiality, integrity, and availability of TODO Customer’s information systems. The findings were categorized by severity level, with TODO SEVERITY RATINGS HERE 0 of the findings being assigned a critical-risk rating, high-risk, 0 medium-risk, and 0 low risk. There were also 1 informational finding related to enhancing security monitoring capabilities within the internal network.

TODO EXECUTIVE SUMMARY HERE

TODO Customer should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. TODO Customer should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that TODO Customer will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

TODO Candidate Name began all testing activities from the perspective of an unauthenticated user on the internet. TODO Customer provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, TODO Candidate Name uncovered a total of 1 findings that pose a material risk to TODO Customer's information systems. TODO Candidate Name also identified 1 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 **1 Info** vulnerabilities were identified:

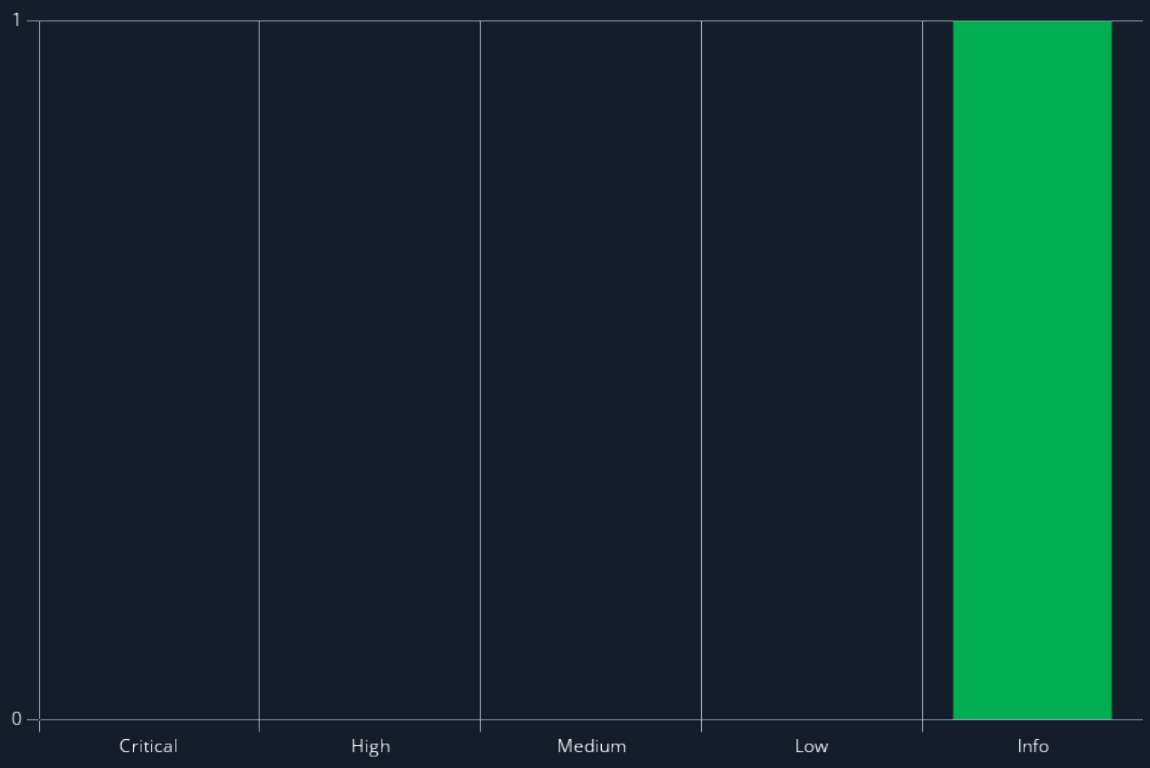

Figure 1 - Distribution of identified vulnerabilities

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	0.0 (Info)	TODO FINDING TITLE	10

5 Internal Network Compromise Walkthrough

During the course of the assessment TODO Candidate Name was able gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over the TODO INSERT DOMAIN NAME Active Directory domain. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details 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.

5.1 Detailed Walkthrough

TODO Candidate Nameperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

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 INTERNAL DOMAIN NAME(S) domain.

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 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.

6.1 Short Term

TODO SHORT TERM REMEDIATION:

- Finding Reference 1 - Set strong (24+ character) passwords on all SPN accounts
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE
- Finding Reference 3 - Enforce a password change for all users because of the domain compromise

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

6.2 Medium Term

TODO MEDIUM TERM REMEDIATION:

- Finding Reference 1 - Disable LLMNR and NBT-NS wherever possible
- 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:

- Perform ongoing internal network vulnerability assessments and domain password audits
- Perform periodic Active Directory security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise
- TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

7 Technical Findings Details

1. TODO FINDING TITLE - Info

CWE	TODO 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 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 TODO Customer's 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 Host & Service 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 Web root	TODO Unrestricted file upload (example)
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

End of Report

This report was rendered
by SysReptor with
♥