<<LOGO EMPRESA CONSULTORA>>

Penetration Test

Report of Findings

**{{project[‘description’]}}**

{{project[‘name’]}}

Version 1.0

Table of Contents

[I. Statement of Confidentiality 1](#_Toc127272000)

[II. Engagement Contacts 2](#_Toc127272001)

[III. Executive Summary 3](#_Toc127272002)

[Approach 3](#_Toc127272003)

[Scope 4](#_Toc127272004)

[Assessment Overview and Recommendations 4](#_Toc127272005)

[IV. Penetration Test Assessment Summary 6](#_Toc127272006)

[Summary of Findings 6](#_Toc127272007)

[V. Technical Findings Details 7](#_Toc127272008)

[VI. Appendices 12](#_Toc127272009)

[Appendix A –Severity Definitions 12](#_Toc127272010)

[Appendix B – Exploited Hosts 13](#_Toc127272011)

[Appendix C – Compromised Users 14](#_Toc127272012)

[Appendix D – Changes/Host Cleanup 15](#_Toc127272013)

[Appendix E – Domain Password Review 16](#_Toc127272014)

# 

# Statement of Confidentiality

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

The contents of this document do not constitute legal advice. HTB Academy’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 HTB Academy external or internal infrastructure.

# Engagement Contacts

|  |  |  |
| --- | --- | --- |
| Customer Contacts | | |
| **Primary Contact** | **Title** | **Primary Contact Email** |
| <<CUSTOMER NAME>> | Chief Executive Officer | rachel@client.local |
| **Secondary Contact** | **Title** | **Secondary Contact Email** |
| <<CUSTOMER NAME>> | Chief Technical Officer | wley@client.local |

|  |  |  |
| --- | --- | --- |
| Assessor Contact | | |
| **Assessor Name** | **Title** | **Assessor Contact Email** |
| {%tr for user\_id in project['testers'] %} | | |
| {{ project['testers'][user\_id][‘fname’] }} {{ project['testers'][user\_id][‘lname’] }} | Security Consultant | {{ project['testers'][user\_id][‘email’] }} |
| {%tr endfor %} | | |

# Executive Summary

{{project[‘description’]}} contracted HTB Academy to perform a Penetration Test of {{project[‘description’]}}’s internally/externally facing network to identify security weaknesses, determine the impact to {{project[‘description’]}}, document all findings in a clear and repeatable manner, and provide remediation recommendations.

## Approach

HTB Academy performed testing under a “{{project[‘scope’]}}” approach May 12, 2022, to May 31, 2022 without credentials or any advance knowledge of {{project[‘description’]}}’s internally 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 via a host that was provisioned specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. HTB Academy sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If HTB Academy were able to gain a foothold in the internal network, {{project[‘description’]}} allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

## Scope

The scope of this assessment is shown in the following table.

In-Scope Assets

|  |  |
| --- | --- |
| Host/URL/IP Address/Domain | Description |
| {%tr for network\_id in networks %} | |
| {{networks[network\_id][‘ip’]}}/{{networks[network\_id][‘mask’]}} | {{networks[network\_id][‘name’]}} |
| {%tr endfor %} | |

Table 1: Scope Details

## Assessment Overview and Recommendations

During the internal penetration test against {{project[‘description’]}}, HTB Academy identified seven (7) findings that threaten the confidentiality, integrity, and availability of {{project[‘description’]}}’s information systems. The findings were categorized by severity level, with one (1) of the findings being assigned a high-risk rating, one (1) medium-risk, and one (1) low risk. There was also one (1) informational finding related to enhancing security monitoring capabilities within the internal network.

<<EXAMPLE: REMOVE UNNECEARY COMMENT>>

The tester found <<CUSTOMER>>’s patch and vulnerability management to be well-maintained. None of the findings in this report were related to missing operating system or third-party patches of known vulnerabilities in services and applications that could result in unauthorized access and system compromise. Each flaw discovered during testing was related to a misconfiguration or lack of hardening, with most falling under the categories of weak authentication and weak authorization.

One finding involved a network communication protocol that can be “spoofed” to retrieve passwords for internal users that can be used to gain unauthorized access if an attacker can gain unauthorized access to the network without credentials. In most corporate environments, this protocol is unnecessary and can be disabled. It is enabled by default primarily for small and medium sized businesses that do not have the resources for a dedicated hostname resolution (the “phonebook” of your network) server. During the assessment, the presence of these resources was observed on the network, so <<CUSTOMER>> should begin formulating a test plan to disable the dangerous service.

The next issue was a weak configuration involving service accounts that allows any authenticated user to steal a component of the authentication process that can often be guessed offline (via password “cracking”) to reveal the human-readable form of the account’s password. These types of service accounts typically have more privileges than a standard user, so obtaining one of their passwords in clear text could result in lateral movement or privilege escalation and eventually in complete internal network compromise. The tester also noticed that the same password was used for administrator access to all servers within the internal network. This means that if one server is compromised, an attacker can re-use this password to access any server that shares it for administrative access. Fortunately, both issues can be corrected without the need for third-party tools. Microsoft’s Active Directory contains settings that can be used to minimize the risk of these resources being abused for the benefit of malicious users.

A webserver was also found to be running a web application that used weak and easily guessable credentials to access an administrative console that can be leveraged to gain unauthorized access to the underlying server. This could be exploited by an attacker on the internal network without needing a valid user account. This attack is very well-documented, so it is an exceedingly likely target can be particularly damaging, even in the hands of an unskilled attacker. Ideally, direct external access to this service would be disabled, but if it cannot be, it should be reconfigured with exceptionally strong credentials that are rotated frequently. <<CUSTOMER>> may also want to consider maximizing the log data collected from this device to ensure that attacks against it can be detected and triaged quickly.

The tester also found shared folders with excessive permissions, meaning that all users in the internal network can access a considerable amount of data. While sharing files internally between departments and users is important to day-to-day business operations, wide open permissions on file shares may result in unintentional disclosure of confidential information. Even if a file share does not contain any sensitive information today, someone may unwittingly put such data there thinking it is protected when it isn’t. This configuration should be changed to ensure that users can access only what is necessary to perform their day-to-day duties.

Finally, the tester noticed that testing activities seemed to go mostly unnoticed, which may represent an opportunity to improve visibility into the internal network and indicates that a real-world attacker might remain undetected if internal access is achieved. <<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. <<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 <<CUSTOMER>> will be able to detect and respond to suspicious activity.

# Penetration Test Assessment Summary

HTB Academy began all testing activities from the perspective of an unauthenticated user on the internal/external network. {{project[‘description’]}} provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

## Summary of Findings

During the course of testing, HTB Academy uncovered a total of four (4) findings that pose a material risk to {{project[‘description’]}}’s information systems. HTB Academy also identified one informational finding that, if addressed, could further strengthen {{project[‘description’]}}’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 {% set criticality = {‘critical’:0,’high’:0,’medium’:0,’low’:0,’info’:0} %}{% for issue\_id in issues %} {% set a = criticality.update({issues[issue\_id][‘criticality’]:(criticality[issues[issue\_id][‘criticality’]]+1)}) %}{% endfor %} | | | | |
| **Critical** | **High** | **Medium** | **Low** | **Total** |
| {% if not criticality[‘critical’] %}0{% else %} {{criticality[‘critical’]}} {% endif %} | {% if not criticality[‘high’] %}0{% else %} {{criticality[‘high’]}} {% endif %} | {% if not criticality[‘medium’] %}0{% else %} {{criticality[‘medium’]}} {% endif %} | {% if not criticality[‘low’] %}0{% else %} {{criticality[‘low’]}} {% endif %} | {% if not criticality[‘critical’] %}0{% else %}{{criticality[‘critical’]}} {% endif %}+{% if not criticality[‘high’] %}0{% else %}{{criticality[‘high’]}} {% endif %}+{% if not criticality[‘medium’] %}0{% else %}{{criticality[‘medium’]}} {% endif %}+{% if not criticality[‘low’] %}0{% else %}{{criticality[‘low’]}} {% endif %} |

Table 2: Severity Summary

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.

|  |  |  |
| --- | --- | --- |
| Finding # | Severity Level | Finding Name |
| {%tr for group\_issue\_name in grouped\_issues %} | | |
|  | {% for issue\_id in grouped\_issues[group\_issue\_name] %}  {{ issues[issue\_id][‘criticality’].replace(‘critical’,’Critical’).replace(‘high’, ‘High’).replace(‘medium’,’Medium’).replace(‘low','Low’) }}  {% endfor %} | {{group\_issue\_name}} |
| {%tr endfor %} | | |

Table 3: Finding List

# Technical Findings Details {% set image\_count = [1] %} {% set text\_count = [1] %} {% for group\_issue\_name in grouped\_issues %}

1. {{group\_issue\_name}}{% for issue\_id in grouped\_issues[group\_issue\_name] %} – {{ issues[issue\_id][‘criticality’].replace(‘critical’,’Critical’).replace(‘high’, ‘High’).replace(‘medium’,’Medium’).replace(‘low','Low’) }}

|  |  |
| --- | --- |
| CWE | CWE-{{ issues[issue\_id][‘cwe’] }} |
| CVSS 3.1 Score | {{ issues[issue\_id][‘cvss’] }} |
| Description | {{ issues[issue\_id][‘description’] }} |
| Security Impact | {{ issues[issue\_id][‘risks’] }} |
| Affected Host/Domain | {% for port\_id in issues[issue\_id]['services'] %}{% if issues[issue\_id]['services'][port\_id]['is\_ip'] %}{{issues[issue\_id]['services'][port\_id]['ip']}}{% if ports[port\_id]['port'] != 0 %}:{{ports[port\_id]['port']}}{% endif %}{% if not loop.last %}  {% elif issues[issue\_id]['services'][port\_id]['hostnames'] %}  {% endif %}{% endif %}{% for hostname\_id in issues[issue\_id]['services'][port\_id]['hostnames'] %}{{hostnames[hostname\_id]['hostname']}}{% if ports[port\_id]['port'] != 0 %}:{{ports[port\_id]['port']}}{% endif %} {% if not loop.last %}  {% endif %} {% endfor %}{% endfor %} |
| Remediation | {{ issues[issue\_id][‘fix’] }} |
| External References | {{ issues[issue\_id][‘references’] }} |

{% if issues[issue\_id][‘pocs’] %}Proof of Concept:{% endif %}

{% if issues[issue\_id][‘pocs’] %}{% for poc\_id in issues[issue\_id][‘pocs’] %}{% if pocs[poc\_id][‘priority’] == 1 %}{% if pocs[poc\_id][‘filetype’]==’text’ %}

| {{ pocs[poc\_id][‘content’] }} |
| --- |

List of code {{text\_count[0]}} - {{pocs[poc\_id][‘comment’]}} {% if text\_count.append(text\_count.pop() + 1) %}{% endif %}{% elif pocs[poc\_id][‘filetype’]==’image’ %}

| {{docx\_image(poc\_id, width=170) }} |
| --- |

Image {{image\_count[0]}}-{{pocs[poc\_id][‘comment’]}} {%if image\_count.append(image\_count.pop()+1) %}{%endif%}{%endif%}{%endif%}{%endfor%}{% endif %}

{%endfor -%}

{%endfor -%}

# Appendices

## Appendix A –Severity Definitions

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based on 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 data.

|  |  |
| --- | --- |
| Rating | Severity Rating Definition |
| **Critical** |  |
| **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. |
| Info |  |

Table 4: Severity Definitions

## Appendix B – Exploited Hosts

|  |  |  |  |
| --- | --- | --- | --- |
| Host | Scope | Method | Notes |
| 192.168.195.204 (DC01) | Internal | DCSync | Domain compromise |
| 192.168.195.205 (MS01) | Internal | Credential Theft (Registry) | Domain lateral movement |
| 192.168.195.205 (MS01) | Internal | Tomcat Manger Weak/Default Credentials | Alternate domain foothold |
| 192.168.195.220 (SQL01) | Internal | NBT-NS/LLMNR Response Spoofing/Kerberoasting | Initial foothold |

Table 5: Exploitation Attempt Details

## Appendix C – Compromised Users

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Type | Method | Notes |
| Example1 | Domain | NBT-NS/LLMNR Response Spoofing/Kerberoasting | Standard Domain User |
| Example2 | Domain | Kerberoasting | Local admin on SQL01 |
| Example3 | Domain | Credential Theft (Registry) | Local admin on all servers |
| Example4 | Domain | Credential Theft (Kerberos TGT Ticket) | Sysadmin with DCSync rights |

Table 6: User Accounts Compromised

## Appendix D – Changes/Host Cleanup

|  |  |  |
| --- | --- | --- |
| Host | Scope | Change/Cleanup needed |
| 192.168.195.205 (MS01) | Internal | WAR file in C:\Program Files (x86)\Apache Software Foundation\Tomcat 10.0\webapps | deploymenttest.war | md5sum: db7d6def7d80b8e982f3359875ea54e3 |
| 192.168.195.205 (MS01) | Internal | JSP file in C:\Program Files (x86)\Apache Software Foundation\Tomcat 10.0\webapps\ deploymenttest | cmd.jsp | md5sum: 5391c4a8af1ede757ba9d28865e75853 |

Table 7: Assessment Artifacts

## Appendix E – Domain Password Review

Password Statistics

|  |  |
| --- | --- |
| Metric | # |
| Total Password Hashes Obtained | 2,000 |
| Total Passwords Cracked | 1,284 |
| % of Passwords Cracked | 64.2 % |
| Number of Domain Admins | 12 |
| Cracked Domain Admin Passwords | 5 |
| % of Domain Admin Passwords Cracked | 42 % |

Table 8: Password Cracking Statistics

Most Commonly Used Passwords

|  |  |
| --- | --- |
| Metric | # |
| BANCO# | 168 |
| Welcome1 | 22 |
| Password123 | 10 |
| Spring2022 | 2 |

Table 9: Password Reuse Statistics

Password Length Breakdown

|  |  |
| --- | --- |
| Length | # |
| 14 | 13 |
| 13 | 10 |
| 12 | 8 |
| 11 | 27 |
| 10 | 38 |
| 9 | 220 |
| 8 | 897 |
| 7 | 67 |

Table 10: Password Length Statistics