

Penetration Test Report

WeakCorp

March 32, 2022

**427 Security**

3359 Mississauga Rd

DH2020

Mississauga, ON L5L 1C6

Tel : 9-999-999-9999

Fax : 0-000-000-0000

Email : 427security@notacompany.com

Web : 427notacompany.com

# Contents

1. **EXECUTIVE SUMMARY……………………………………………………………………..3**
   1. SUMMARY OF RESULTS………………………………………………………..….3
2. **SCOPE OF TESTING………………………………………………………………………...4**
   1. FEATURES TO BE TESTED………………………………………………………..4
   2. FEATURES NOT TO BE TESTED………………………………………………….4
3. **ASSUMPTIONS……………………………………………………………………………….4**
4. **TEST COMPLETION CRITERIA…………………………………………………………….5**
5. **TESTING STRATEGY………………………………………………………………………...5**
6. **TEST RESULTS……………………………………………………………………………….6**
7. **TOOLSET………………………………………………………………………………………8**
8. **CONCLUSION…………………………………………………………………………………9**
   1. RECOMMENDATIONS……………………………………………………………….9

## EXECUTIVE SUMMARY

427 Security was contracted by WeakCorp to conduct a penetration test in order to determine its system’s vulnerabilities to malicious attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against WeakCorp with the goals of:

* Identifying if a remote attacker could penetrate WeakCorp’s cybersecurity defenses.
* Determining the impact of a security breach on WeakCorp’s private data.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 (<https://csrc.nist.gov/publications/detail/sp/800-115/final>).

## SCOPE OF TESTING

### A. FEATURES TO BE TESTED

Personnel employed by *427 Security* may test any of the following services running on

the client’s system:

1. Samba Servers
2. MySQL Server

### B. FEATURES NOT TO BE TESTED

Personnel employed by *427 Security* are prohibited from testing the following:

1. Any service not mentioned in the previous section.
2. The operations security (OPSEC) of the organization
   1. Using techniques such as social engineering on WeakCorp personnel is prohibited

## ASSUMPTIONS

Before starting to test, the following conditions should be met:

* The test environment is ready and configured appropriately
  + The employee has a “Kali Linux” virtual machine installed on their system
* The employee is able to access WeakCorp servers
  + The “servers” can be accessed by cloning the following GitHub repository and following the [instructions](https://github.com/bjelefano/CSC427Winter2022-MetasploitLab/blob/main/CSC427_Lab_Instructions.pdf) provided for the lab assignment:
  + <https://github.com/bjelefano/CSC427Winter2022-MetasploitAssignment>

## TEST COMPLETION CRITERIA

The testing process must cease immediately if any of the following conditions are met:

* A critical vulnerability has been found in each of the services outlined section 2
* The due date has been passed, and all grace tokens have been used

## TESTING STRATEGY

**TO-DO: Give a brief, step-by-step overview on how you used Metasploit to test the client’s system.**

## 

## TEST RESULTS

**TO-DO: Report the details of 2 vulnerabilities that you found in the system. Include a screenshot, if any, as a proof. (1-2 sentences for “Details of Vulnerability” and “Impacts”)**

1. **Vulnerability Title :**

**CVE Number :**

**Severity (CVSS) :**

**Details of Vulnerability :**

**Impacts :**

**Screenshot(s):**

1. **Vulnerability Title :**

**CVE Number :**

**Severity (CVSS) :**

**Details of Vulnerability :**

**Impacts :**

**Screenshot(s):**

## 

## TOOLSET

**TO-DO: Complete the list below with all the metasploit modules/encoders you used during the penetration testing, and explain the purpose of the module in 1 sentence.**

**Name:** auxiliary/fuzzers/ssh/ssh\_version\_15 (EXAMPLE)

**Description:** SSH 1.5 Version Fuzzer

**Purpose:**

1. **Name:**

**Description:**

**Purpose:**

1. **Name:**

**Description:**

**Purpose:**

1. **Name:**

**Description:**

**Purpose:**

## 

## CONCLUSION

**TO-DO: Write 1-2 paragraphs summarizing all your findings and the overall security of the WeakCorp (hint: check our references)**

### RECOMMENDATIONS

Due to the impact to the overall organization as uncovered by this penetration testing, 427 Security recommends the following:

**TO-DO: Write at least 3 recommendations that WeakCorp needs to do based on your findings.**



## REFERENCES

1. <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>
2. <https://www.sam-solutions.com/blog/wp-content/uploads/2017/03/Security-test-plan-template.pdf>
3. <https://www.getastra.com/blog/wp-content/uploads/2021/06/Astra-Security-Sample-VAPT-Report.pdf>