# **Comprehensive Cybersecurity Report: Vulnerability Assessment and Remediation**

Date: 29 september 2023

**Executive Summary**

Dear Sir,

I hope this report finds you well. As a cybersecurity researcher, my primary goal is to ensure the security of your systems and data. During my recent assessment, I conducted three tests to evaluate the security of your server environment. This report is designed to provide you with a clear understanding of the findings, steps taken, and recommended actions in both a technical and non-technical manner.

**Overview**

**Vulnerability Overview**

The tests conducted revealed vulnerabilities in your server environment, specifically in the Metasploitable2 machine. These vulnerabilities include:

**1. FTP BruteForce Vulnerability:** The Metasploitable2 machine is vulnerable to FTP brute force attacks, which could lead to unauthorized access.

**2. SSH BruteForce Vulnerability:** The SSH service on the Metasploitable2 machine is susceptible to brute force attacks, potentially compromising system security.

**3. Unreal IRC Exploitation:** The Unreal IRC service on the Metasploitable2 machine is exploitable, allowing unauthorized access to the system.

**Overall Risk Rating:**

After a comprehensive assessment, the overall risk rating for these vulnerabilities is High. This indicates the severity and potential impact of these issues on your systems and data.

**Prioritized Recommendations**

**Recommendations for Action**

To address the identified vulnerabilities, we have prioritized the following recommendations:

• **FTP BruteForce Vulnerability:**

◇ Patch and Update: Update the FTP service and apply patches to eliminate the vulnerability.

◇ Access Control: Implement stringent access control mechanisms to restrict unauthorized access.

◇ Security Awareness: Educate your team about cybersecurity best practices to recognize and report potential threats.

• **SSH BruteForce Vulnerability:**

◇ Patch and Update: Update the SSH service and apply patches to mitigate the risk.

◇ Strong Password Policies: Enforce strong password policies to reduce the effectiveness of brute force attacks.

◇ Intrusion Detection: Deploy intrusion detection systems to monitor and block suspicious SSH login attempts.

• **Unreal IRC Exploitation:**

◇ Patch and Update: Update the Unreal IRC service to the latest version to close the known vulnerabilities.

◇ Network Segmentation: Isolate the Metasploitable2 machine from critical systems to minimize potential damage.

◇ Incident Response Plan: Develop an incident response plan to react swiftly in case of a breach.

**Test Scope and Method**

**Extent of Testing**

The scope of our testing encompassed various attack scenarios, including FTP and SSH brute force attacks, as well as the exploitation of the Unreal IRC service.

**Internal Phase**

During the internal testing phase, we assessed the vulnerabilities present on the Metasploitable2 machine using the tools and techniques described in the respective test reports.

**External Phase**

The external testing phase involved simulating attacks from external sources to evaluate system resilience.

**Conclusions**

**Most Likely Compromise Scenarios**

Based on our assessment, the most likely compromise scenarios include unauthorized access to the Metasploitable2 machine, potentially leading to data breaches or system compromise.

**Implications**

The implications of these vulnerabilities include potential data loss, system downtime, and damage to your organization's reputation.

**References**

To support our findings, we refer to the following resources:

◇ Test 1: FTP BruteForce Test [<https://github.com/mdomorffaruk/hack_ms2_in_many_ways/blob/master/ftp_ms2.md>]

◇ Test 2: SSH BruteForce Test [<https://github.com/mdomorffaruk/hack_ms2_in_many_ways/blob/master/ssh_bruteforce_ms2.md>]

◇ Test 3: Unreal IRC Exploitation Test [<https://github.com/mdomorffaruk/hack_ms2_in_many_ways/blob/master/unreal_irc_ms2.md>]

◇ Github Repository Link: [<https://github.com/mdomorffaruk/hack_ms2_in_many_ways/tree/master>]

Your server's security is of paramount importance, and addressing these vulnerabilities is crucial to safeguard your data and systems. I am here to assist you in implementing the recommended actions and providing ongoing support to ensure the security of your infrastructure.

If you have any questions or require further clarification on any aspect of this report, please do not hesitate to reach out. Together, we can strengthen your cybersecurity defenses and mitigate potential risks effectively.