

Penetration Test Report

MegaCorp One

April 28th, 2023

**Luke Perri Industries, LLC**

111 Lake Hollingsworth Drive

Apt. Garden A

Lakeland, FL 33801

United States of America

Phone: 239-302-8660

Fax: 610-252-6534

Email: [lukeperri71@gmail.com](mailto:lukeperri71@gmail.com)

Web: [https://lukeperriindustries.com](https://lukeperri.com)

Table of Contents

[**Executive Summary 1**](#_oqdzg5j8o0cs)

[*Summary of Result 1*](#_w55305c7o0w7)

[**Attack Narrative 2**](#_89qf02bspgzl)

[*NMAP scan of Axigen 2*](#_kg9xeic04uu)

[*Nessus Scan of Axigen 2*](#_g7hzgawp7vu8)

[*NMAP scan on Metasploitable 3*](#_gg48pc1vkjrf)

[*Enumeration scan on Metasploitable 4*](#_yyp0a8kf7rsi)

[*Nessus scan on Metasploitable 6*](#_pj1rhfpwrld5)

[*11356 - NFS Exported Share Information Disclosure 7*](#_wu8i2dmdlcbv)

[*134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat) 8*](#_gpma4ufs38ht)

[**Conclusion 10**](#_fio6cxv3anhp)

[**Appendix A 10**](#_yh5h0h6a3gm7)

[**Appendix B 10**](#_x6c2bv0bff9)

# 

# Executive Summary

This report details the findings of the penetration test conducted on MegaCorp One by Luke Perri Industries between April 17th, 2023, and April 29th, 2023. The objective of the penetration test was to identify and exploit vulnerabilities on the company's Axigen web server and Metasploitable server. The methods used to conduct this were a combination of NMAP scans, enumeration scans, and vulnerability scans.

## Summary of Result

After conducting scans of the Axigen server a few minor vulnerabilities were found that should be addressed as soon as possible. One such vulnerability leaves traffic on the network open to attackers being able to learn users' usernames and passwords. However, the server is mostly well-secured and impervious to most attacks.

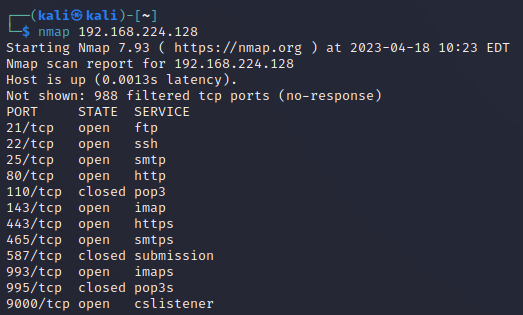
On the other hand, the Metasploitable server is much more vulnerable. During the vulnerability scan, we identified over 100 vulnerabilities. Since such a large number of vulnerabilities were found, we decided to only exploit the most critical ones. One such vulnerability allows us to plant files directly into the Metasploitable directory. While another allowed files from the web server to be read.

# 

# Attack Narrative

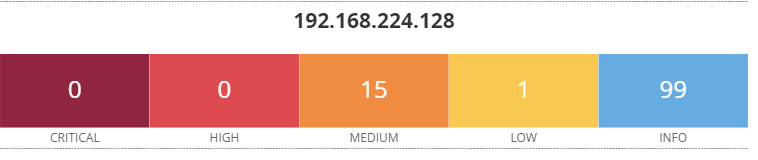
## NMAP scan of Axigen

The NMAP scan of the Axigen revealed a few open ports. Given ports 80 and 443, it could be determined that the IP belonged to a web server.



## Nessus Scan of Axigen

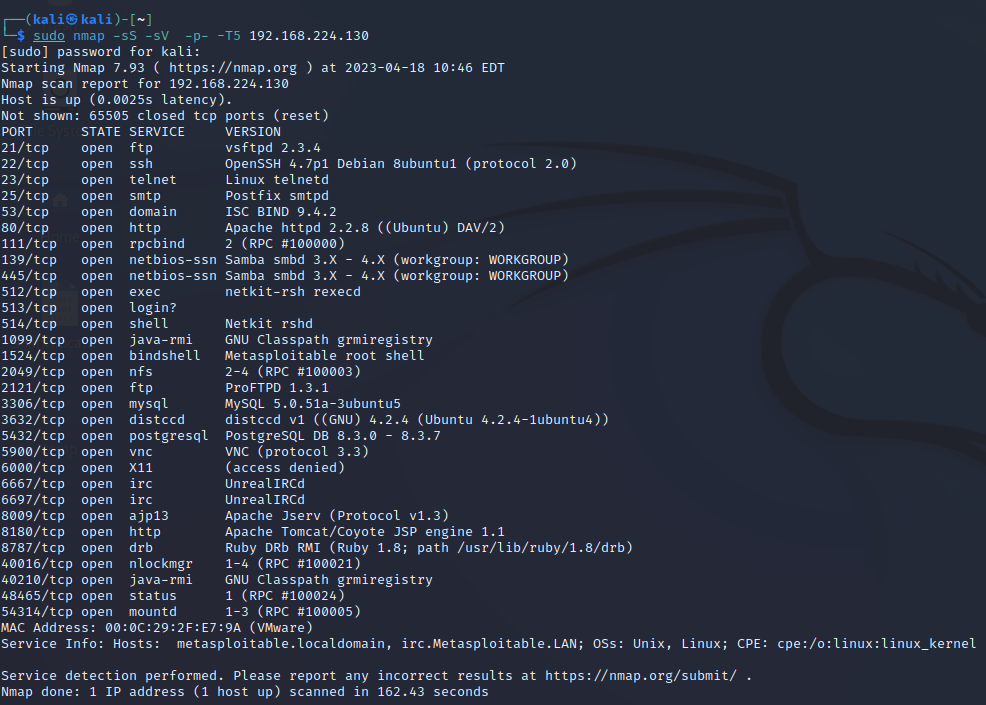
Conducting a vulnerability scan revealed a few vulnerabilities with a medium CVE score, however, none of them proved critical to the system.



## 

## NMAP scan on Metasploitable

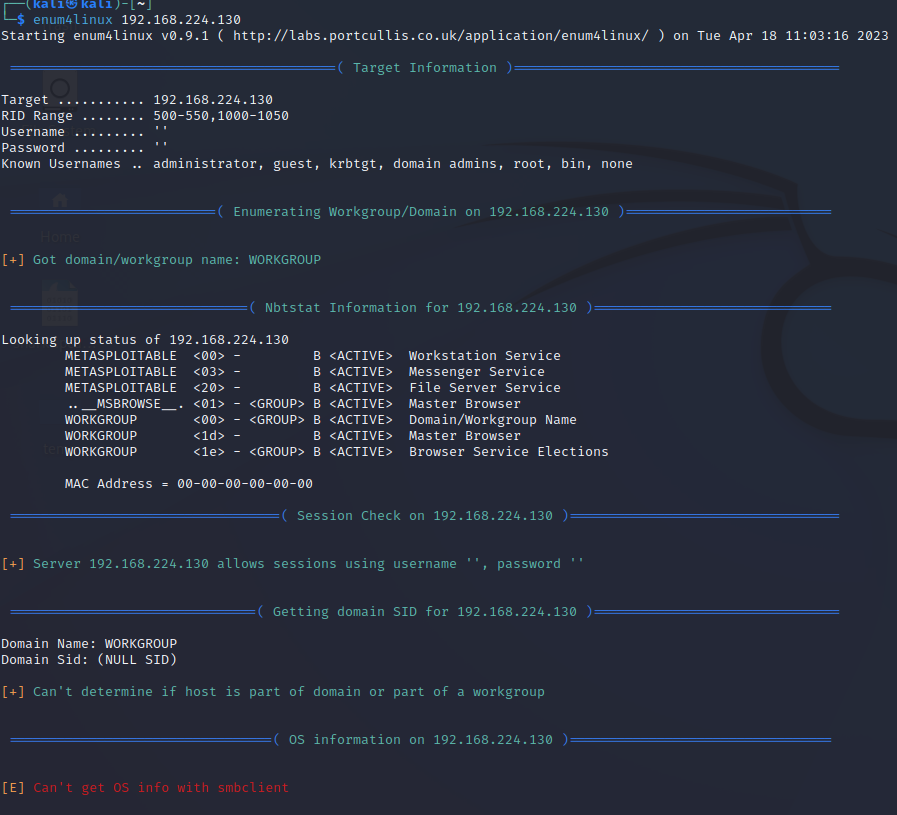
To begin finding vulnerabilities an NMAP scan was first done on the Metasploitable system. The results show the open ports on the network which were later used in conjunction with the results from the Nessus scan to exploit the vulnerabilities found on the system.



## 

## Enumeration scan on Metasploitable

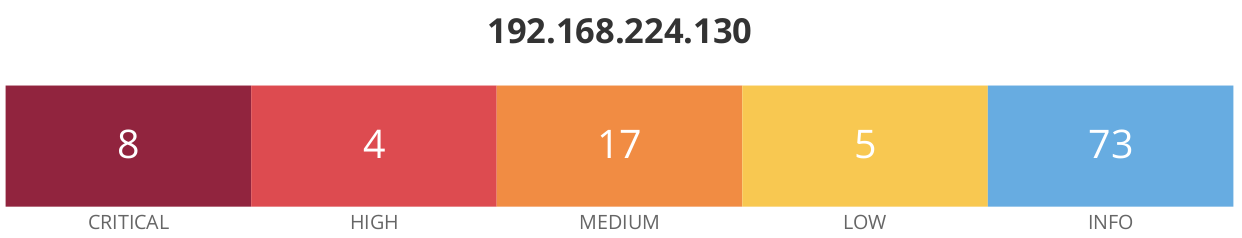
While not much new information was found from the enumeration scan of the network, it was able to identify what type of server the IP belonged to as well as the server’s password policy. This could be vital for allowing attackers to narrow down the possible passwords for the domain.



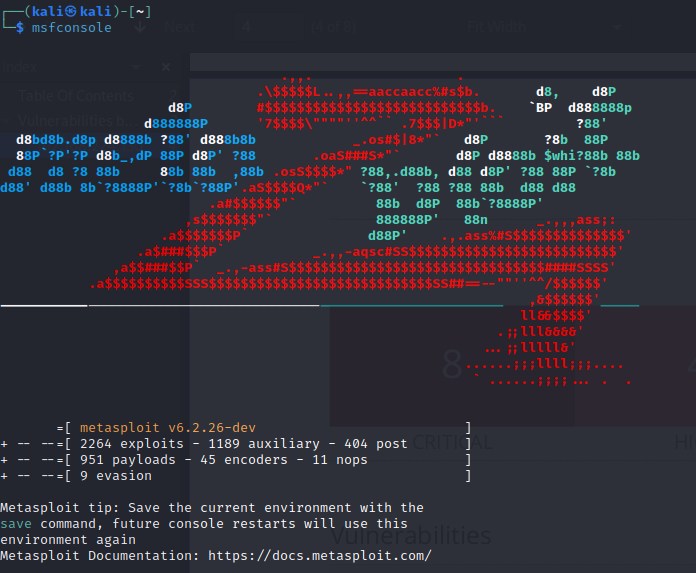
## 

## 

## Nessus scan on Metasploitable

The Nessus scan highlighted many vulnerabilities on the Metasploitable server. A total of 107 vulnerabilities were found with eight of them having either a critical or high CVE score.

After getting a list of the vulnerabilities we accessed the Metasploit console to exploit some of the vulnerabilities found.



### 11356 - NFS Exported Share Information Disclosure

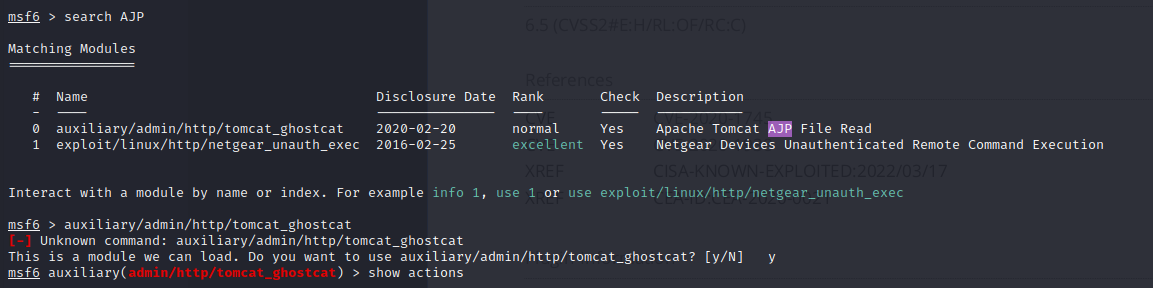
One critical vulnerability was being able to access NFS shares on a remote host. With this vulnerability, you mount the Metasploitable file directory to your own files. From there you are able to view, edit, or plant files into Metasploitable. As seen below we were able to plant a text file called Luke.txt using simple commands.

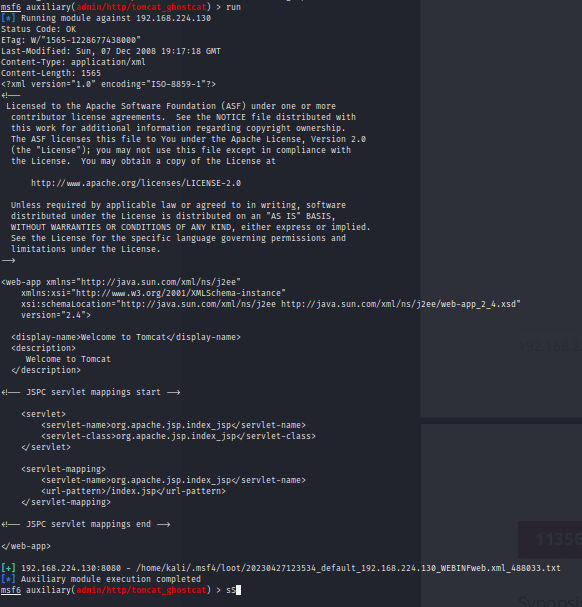
### 

### 

### 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

The next vulnerability allowed attackers to read files from a web server. We were able to search for the module in the Metasploit console and load it. And after running the exploit it was able to retrieve the HTML files from the server.





# 

# Conclusion

In conclusion this penetration test has provided crucial insight into the security of MegaCorp One’s Axigen and Metasploitable server. This test was able to identify many vulnerabilities affecting the servers that could potentially be exploited by attackers. We highly recommend that your company take the time to address each vulnerability to better improve the security of your systems and data. This may include applying the necessary patches to servers or updating configurations to limit access or permissions of users. Routine penetration tests are always important to improving the safety and security of your network and systems.