Top Notch Security

By Tyler Rollinson

2024 Security Assessment Report Prepared For

Hamel Industries

Report Issued: 12/13/2024

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to Mr. Hamel or facilitate attacks against Mr. Hamel. Top Notch Security shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on Mr.Hamel’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[**EXECUTIVE SUMMARY**](#_ybi9gz2s4don)5

[Open Port Recommendation](#_xi9pwbdo96zs) 5

[**HIGH LEVEL ASSESSMENT OVERVIEW**](#_vrxmgfhvd2vy)6

[Observed Security Strengths](#_hbll3idtj3mt) 6

[Areas for Improvement](#_8scnpo1z4bcx) 6

[Short Term Recommendations](#_3wlz3a5xsr9u) 6

[Long Term Recommendations](#_kjl6c96bkl8) 6

[**SCOPE**](#_si0wj5j15p77)7

[Networks](#_ivezkd6kiocx) 7

[Other](#_nzuakwsdt6rt) 8

[Provided Credentials](#_1guor7qepakl) 8

[**TESTING METHODOLOGY**](#_dam9lby6qdj3)10

[**CLASSIFICATION DEFINITIONS**](#_4cbm8he7gc1m)11

[Risk Classifications](#_s6qypp4zj5nq) 11

[Exploitation Likelihood Classifications](#_lruj9twjesc2) 11

[Business Impact Classifications](#_uqxr1e88ekga) 12

[Remediation Difficulty Classifications](#_sm4k0lgedf14) 12

[**ASSESSMENT FINDINGS**](#_5s0202lc8e79)13

[**APPENDIX A - TOOLS USED**](#_g7cophwnkg9g)28

[**APPENDIX B - ENGAGEMENT INFORMATION**](#_kzx5oj6hc3zc)29

[Client Information](#_veb77t36itfa) 29

[Version Information](#_zew1fi62hkvd) 29

[Contact Information](#_mmygx7611ii0) 29

# 

# EXECUTIVE SUMMARY

Tyler Rollinson performed a security assessment of the internal corporate network of Mr.Hamel on 12/1/2024. Top Notch Security’s penetration test simulated an attack from an external threat actor attempting to gain access to systems within Mr.Hamel’s corporate network. The purpose of this assessment was to discover and identify vulnerabilities in Mr.Hamel’s infrastructure and suggest methods to remediate the vulnerabilities. We identified a total of 80+ vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| **30** | **20** | **20** | **10** |

The highest severity vulnerabilities give potential attackers the opportunity to gain access from an open port, SQL injections or Metasploit framework exploits. This issue along with outdated versions of software could create a problem where they can create accounts, crack passwords, and gain access to databases. From this point, they can then gain more information and access more of your systems, and overall compromise your whole infrastructure if they are not addressed. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

Tyler Rollinson identified the following strengths in Mr. Hamels s network which greatly increases the security of the network. Mr. Hamel should continue to monitor these controls to ensure they remain effective.

Changing Passwords

* The passwords that were used to gain access previously were changed on a routine basis.

## Areas for Improvement

Top Notch Security recommends Mr. Hamel take the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack Mr. Hamel’s information systems and/or reduce the impact of a successful attack.

### Short Term Recommendations

Tyler Rollinson recommends Mr. Hamel take the following actions as soon as possible to minimize business risk.

* Close open ports that are not needed
* Routine scans to check network activity

### Long Term Recommendations

Tyler Rollinson recommends the following actions be taken over the next 3 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

Implement network segmentation

Enable multi-factor authentication

Create a firewall for your networks

Update all your systems to the most recent or secure updates

Change all passwords routinely

Add anti-malware software

# 

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

## Networks

|  |  |
| --- | --- |
| **Network** | **Note** |
| 192.168100.0/24 | Network for Corporate HQ |
| 192.168.100.101 | Office Computer |
| 192.168.100.108 | Office Computer |
| 192.168.100.109 | CEO Computer |
| 192.168.100.115 | Office Computer |
| 192.168.100.116 | Office Computer |
| 192.168.100.117 | Office Computer |
| 192.168.100.118 | Office Computer |
| 192.168.100.119 | Office Computer |
| 192.168.100.120 | Office Computer |
| 192.168.100.124 | Office Computer |
| 192.168.100.124 | Office Computer |
| 192.168.100.125 | Office Computer |
| 192.168.100.197 | Office Computer |
| 192.168.100.210 | Office Computer |
| 192.168.100.211 | Office Computer |
| 192.168.100.217 | Office Computer |

## Other

|  |  |  |
| --- | --- | --- |
| **Name** | **System Type** | **Note** |
| IVR System | Phone | 555-555-1234 |

## Provided Credentials

Mr.Hamel provided Top Notch Security with the following credentials and access to facilitate the security assessment listed below.

|  |  |
| --- | --- |
| **Item** | **Note** |
| Customer Account | BestJedi@fakemail.com |
| IVR Testing Phone | (555-555-5678) Specific phone to use for IVR system testing. |

# 

# TESTING METHODOLOGY

Tyler Rollinson’s testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about Mr.Hamel’s network systems. We used port scanning and other enumeration methods like -sV and -sC scans to refine target information and assess target values. Next, we conducted our targeted assessment. We simulated an attacker exploiting vulnerabilities in Mr.Hamel’s network by using Metasploit exploits and password cracking software as some examples. Tyler Rollinson gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.

# 

# CLASSIFICATION DEFINITIONS

## Risk Classifications

|  |  |  |
| --- | --- | --- |
| **Level** | **Score** | **Description** |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

|  |  |
| --- | --- |
| **Likelihood** | **Description** |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

|  |  |
| --- | --- |
| **Impact** | **Description** |
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

|  |  |
| --- | --- |
| **Difficulty** | **Description** |
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

## 

# ASSESSMENT FINDINGS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Number** | **Finding** | **Risk Score** | **Risk** | **Page** |
| 1 | Example Vulnerability Finding | **9** | **High** | 11 |
| 2 | Firewall Rule Set Not Best Practice | **8** | **High** | 12 |
| 3 | Outdated Software | **6** | **Medium** | 69 |
| 4 | Multiple XYZ Vulnerabilities | **5** | **Medium** | 420 |
| 5 | Fake Finding | **2** | **Low** | 6969 |

TEMPLATE NOTE: (Sorting by descending risk score)

**1 - Vulnerability Finding**

|  |  |
| --- | --- |
| **HIGH RISK (8/10)** | |
| **Exploitation Likelihood** | **Severe** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Open ports for most of the IP’s on the office network along with outdated versions.

**Analysis**

When I performed a port scan on the Office HQ network, most of the office computers had open ports that could be exploited gain access. When I performed an -sV scan, most of the versions were outdated. If this is not fixed with the proper response, the network security will continue to be compromised and risk exploitation on a daily occurrence. This would be detrimental to the productivity of your company.

Below are screenshots of the target computers with open ports and their versions.

192.168.100.108

OS-Microsoft Windows 8.1 R1

A screenshot of a computer program

Description automatically generated

192.168.100.109

OS- Linux 2.6.9-2.6.33

A screenshot of a computer

Description automatically generated

192.168.100.115

OS-Linux 3.12 – 4.10

A screenshot of a computer

Description automatically generated

192.168.100.116

OS – Linux 2.6.32 – 3.10

A screenshot of a computer

Description automatically generated

192.168.100.117

OS- Linux 2.6.32

A screenshot of a computer

Description automatically generated

192.168.100.118

OS – Linux 3.2 – 4.9

A screenshot of a computer

Description automatically generated

192.168.100.119

OS – Linux 2.6.9 – 2.6.33

A screenshot of a computer

Description automatically generated

192.168.100.120

OS – Linux 2.6.32 – 3.10

A screenshot of a computer

Description automatically generated

192.168.100.123

OS – Linux 5.1

A screenshot of a computer

Description automatically generated

192.168.100.124

OS – Linux 2.6.32 – 3.10

A screenshot of a computer

Description automatically generated

192.168.100.125

OS – FreeBSD 11.2-RELEASE

A screenshot of a computer

Description automatically generated

192.168.100.197

OS – FreeBSD 11.2-RELEASE

A screenshot of a computer

Description automatically generated

192.168.100.210

OS- Linux 5.1

A screenshot of a computer

Description automatically generated

192.168.100.211

OS- Linux 5.1

A screenshot of a computer

Description automatically generated

192.168.100.217

OS – Linux 5.1

A screenshot of a computer

Description automatically generated

Screenshot of 192.168.100.118 -sC scan.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Recommendations**

* Close unneeded ports that are open.
* If this is not possible do routine network scans to monitor activity.
* Update Operating Systems and Versions of software.

**2 - Vulnerability Finding**

|  |  |
| --- | --- |
| **HIGH RISK (8/10)** | |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Gained access to a web browser through an employee account. I also gained access to an admin account for 192.168.100.119 DVWA site.

**Analysis**

When I performed a port scan on the ip 192.168.100.217 I found that it had open ports that could be exploited. I decided to input the ip into a web browser and found that it had a website with a login page. From there, I did an os scan, and version scan. I then proceeded to use HydraX, a password cracking tool and was able to gain access. I used the same process for 192.168.100.119 to gain access to the admin account.

Below are screenshots of the process I followed.

-o scan of ip target 217A screenshot of a computer

Description automatically generated

Version scan of the target ip 217A screenshot of a computer

Description automatically generated

Screenshots of getting login for jsmith using a passowrd cracker.

A screenshot of a computer program

Description automatically generated

Screenshot of logging into jsmiths account.

A screenshot of a computer

Description automatically generated

Screenshot of 192.168.100.119 access.

A screenshot of a computer

Description automatically generated

**Recommendations**

* Create two-step authentication/verification
* If that is not possible, Create/ change passwords routinely

**3 - Vulnerability Finding**

|  |  |
| --- | --- |
| **Medium Risk (6/10)** | |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Medium** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Gained access to file servers on IP 192.168.100.117 and 192.168.100.119 using filezilla.

**Analysis**

This poses a medium security threat. I gained access to sensitive information that I should not be able to access. Once I gain access the back end of the file servers, I can obtain sensitive data, upload malicious files or more that could impact business productivity.

Below are screenshots of the file servers in order from 117 to 119

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Recommendations**

* Disable standard ftp
* Use strong passwords, encryption, and hashing
* Implement IP black and whitelists

**4 - Vulnerability Finding**

|  |  |
| --- | --- |
| **Medium Risk (6/10)** | |
| **Exploitation Likelihood** | **Medium** |
| **Business Impact** | **Medium** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

I used Metasploit framework on 192.168.100.119 to initiate a reverse tcp shell.

**Analysis**

This poses a medium security threat. Once I created the reverse shell, I had control over the target computer. This can be a severe issue if it is not addressed. I could execute commands to give me access to the root or admin user. I could also use scripts or other toolkits to take sensitive data or other malicious things.

**Recommendations**

* Upgrade firewall and network security
* Endpoint hardening which entails disabling unnecessary services and have stong SSH passwords.
* Add anti-malware software to help protect from attacks

# APPENDIX A - TOOLS USED

|  |  |
| --- | --- |
| **TOOL** | **DESCRIPTION** |
| **BurpSuite Community Edition** | Used for testing of web applications. |
| **Legion/xhydra** | Used for exploitation of vulnerable services and vulnerability scanning. |
| **Nmap** | Used for scanning ports on hosts. |
| **Legion** | Used to scan the networks for vulnerabilities. |
| **PostgreSQL Client Tools** | Used to connect to the PostgreSQL server. |
| **Nessus** | Gives a vulnerability report of the IP |

***Table A.1:*** *Tools used during assessment*

# APPENDIX B - ENGAGEMENT INFORMATION

## Client Information

|  |  |
| --- | --- |
| **Client** | Mr.Hamel |
| **Primary Contact** | Rick Sanchez, Manager |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement   * Mr.Hamel * John Smith |

## Version Information

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | 12/13/2024 | Initial report to client |

## Contact Information

|  |  |
| --- | --- |
| **Name** | Top Notch Security |
| **Address** | 1001 Fake Street, Gotham, NY 11201 |
| **Phone** | 555-185-1782 |
| **Email** | tylerr@fakemail.com |