**Sedna Industries Inc.**

**Security Assessment Report**

**Business Confidential**

**7/15/2023**

**Table of Contents**

Contents

[Assessment Overview 2](#_Toc140349579)

[Assessment Components 2](#_Toc140349580)

[OSINT 2](#_Toc140349581)

[Internal Penetration Test 2](#_Toc140349582)

[Finding Severity Ratings 2](#_Toc140349583)

[Risk Factors 2](#_Toc140349584)

[Scope 2](#_Toc140349585)

[Executive Summary 2](#_Toc140349586)

[Technical Findings 2](#_Toc140349587)

# Assessment Overview

From July 9th, 2023 to July 11th, 2023, Sedna Industries Inc. commissioned < Company Name>conduct a comprehensive examination of the security posture of one of its internal networks. The methodologies deployed in this rigorous exercise were drawn from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115 guidelines for penetration testing, supplemented by the use of custom frameworks designed to offer additional granularity and depth of insights.

The testing process was conducted in distinct stages, with a focus on Planning, Enumeration, Vulnerability Scanning, Exploitation, and Reporting. Each stage was crucial to provide a thorough assessment of potential vulnerabilities and threats, with the goal of strengthening the overall security profile of the assessed network infrastructure.

# Assessment Components

## OSINT

The Open-Source Intelligence (OSINT) component of the assessment involved the systematic collection and analysis of information from publicly available sources. A range of digital tools were utilized to gather data from sources such as websites, forums, social media platforms, and databases. This data was analyzed to identify potential vulnerabilities and threat vectors, and to gain a deeper understanding of the security posture of Sedna Industries Inc.'s internal networks.

## Internal Penetration Test

The internal penetration test was designed to simulate the activities of an attacker who has successfully breached the initial defense perimeters of the network. The assessment involved a multi-faceted approach, combining several methodologies to ensure a thorough evaluation of potential security weaknesses.

Key stages of the internal penetration testing included:

1. **Vulnerability Scanning**: Automated tools were used to scan the internal network for known vulnerabilities that could potentially be exploited by an attacker. These tools provided a broad overview of potential weaknesses in the network's security.
2. **Threat Modeling**: In this stage, potential threats to the network were identified and modeled based on the vulnerabilities found during the scanning phase. This helped to understand the potential impact of a successful attack on the network.
3. **Exploitation**: Various techniques were used to exploit the identified vulnerabilities in a controlled manner. This provided practical insights into how an attacker could potentially exploit these vulnerabilities and the potential damage that could be caused.
4. **Post-Exploitation**: Once the vulnerabilities were successfully exploited, further testing was conducted to identify what additional access or data an attacker could obtain.
5. **Reporting**: A comprehensive report was created, detailing the vulnerabilities found, their potential impact, and recommended remediation strategies.

# Finding Severity Ratings

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS v3 Score Ranges** | **Score Definition** |
| **Critical** | 9.0 - 10.0 | Critical vulnerabilities indicate that the software could be easily exploited by an attacker and potentially result in a total compromise of the system's confidentiality, integrity, or availability. |
| **High** | 7.0 - 8.9 | High vulnerabilities are significant flaws that could be exploited by an attacker to affect the confidentiality, integrity, or availability of the system but have some mitigating factors that lower the risk compared to critical vulnerabilities. |
| **Medium** | 4.0 - 6.9 | Medium vulnerabilities represent noticeable weaknesses in the system, though an attacker would likely face obstacles in attempting to exploit these vulnerabilities. |
| **Low** | 0.1 - 3.9 | Low vulnerabilities represent minor weaknesses that either offer only limited potential for harm or would be particularly challenging for an attacker to exploit. |
| **Informational** | 0.0 | Informational findings do not pose a security risk but may be useful to attackers for gaining information about the system or planning further attacks. |

# Risk Factors

Risk factors in cybersecurity assessments are typically categorized into two main types: likelihood and impact.

**Likelihood**: This refers to the probability that a specific threat will exploit a particular vulnerability. It takes into account various elements such as the capability of the potential attacker, the existence of the vulnerability, and the presence or absence of countermeasures. Likelihood can be rated on a scale, for instance, low, medium, or high.

**Impact**: This refers to the potential consequences if a vulnerability were to be exploited. Impact can affect various aspects of the organization, including financial loss, reputation damage, legal implications, or operational disruption. Similar to likelihood, impact can be categorized into low, medium, or high.

Together, these two factors (likelihood and impact) create a risk rating that can help prioritize which vulnerabilities need to be addressed first.

# Scope

|  |  |
| --- | --- |
| **Assessment Component** | **Focus Area(s)** |
| OSINT | <https://sednaindustries.com> |
| Internal Penetration Test | 192.168.220.0/24 |

**Scope Exclusions**

During the engagement, Sedna Industries set specific boundaries for the assessment. These exclusions include:

* No social engineering tactics were to be employed.
* Denial of Service (DoS) attacks were explicitly out of scope.

**Method Allowances**

Sedna Industries granted permission for the use of advanced techniques including:

* The use of Generative AI solutions in the assessment process.

# 

# Executive Summary

Between July 9th and July 11th, 2023, Sedna Industries engaged <Company name > to conduct a comprehensive security assessment of one of its internal networks. Spanning a period of five business days, the test's scope was within parameters set by Sedna Industries and aimed to uncover vulnerabilities and evaluate the overall security posture of the network environment.

In the subsequent sections of this report, we detail the discovered vulnerabilities, the strengths and weaknesses of the client's environment, and the specific considerations provided by the client. Furthermore, the report underscores the relevance of these findings in the context of industry-standard guidelines and the evolving cybersecurity landscape.

**Testing Summary**

**<Insert details for testing summary such as tools, tactics and techniques used to assess the client environment>**

**Assessor Notes & Primary Recommendations**

The assessment suggests that Sedna Industries reflects characteristics typical of organizations going through initial security penetration testing engagements. The vulnerabilities discovered primarily fall within common web application security flaws, namely Unrestricted File Upload and Local Privilege Escalation via chkrootkit software.

< Company Name> recommends Sedna Industries conducts a thorough review of its web application security measures, particularly focusing on the OWASP Top 10 Risk factors. This list, compiled by cybersecurity experts worldwide, comprises the most critical web application security risks and provides valuable guidelines for securing a network environment.

Moreover, internal reviews of the software inventory installed on internal hosts should be performed to identify unapproved or potentially unwanted applications. This proactive measure will further fortify the internal network against potential security breaches.

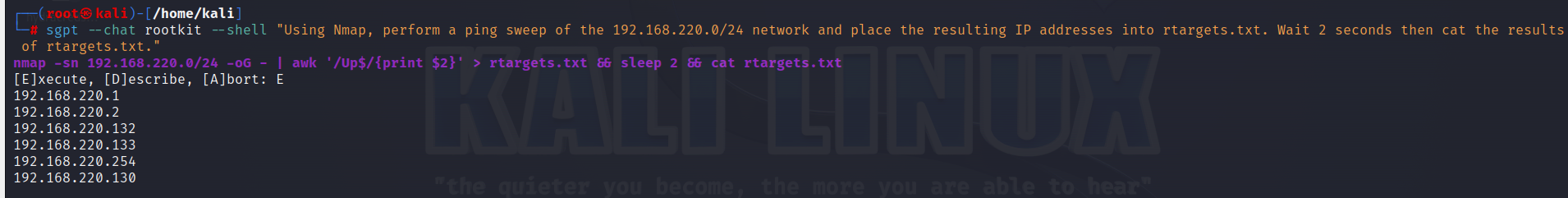
In sum, this assessment is the initial step towards a more robust and resilient security posture for Sedna Industries. By addressing these vulnerabilities and continuing to prioritize security, Sedna Industries will be well-positioned to mitigate future cyber threats.

**Key Strengths and Opportunities**

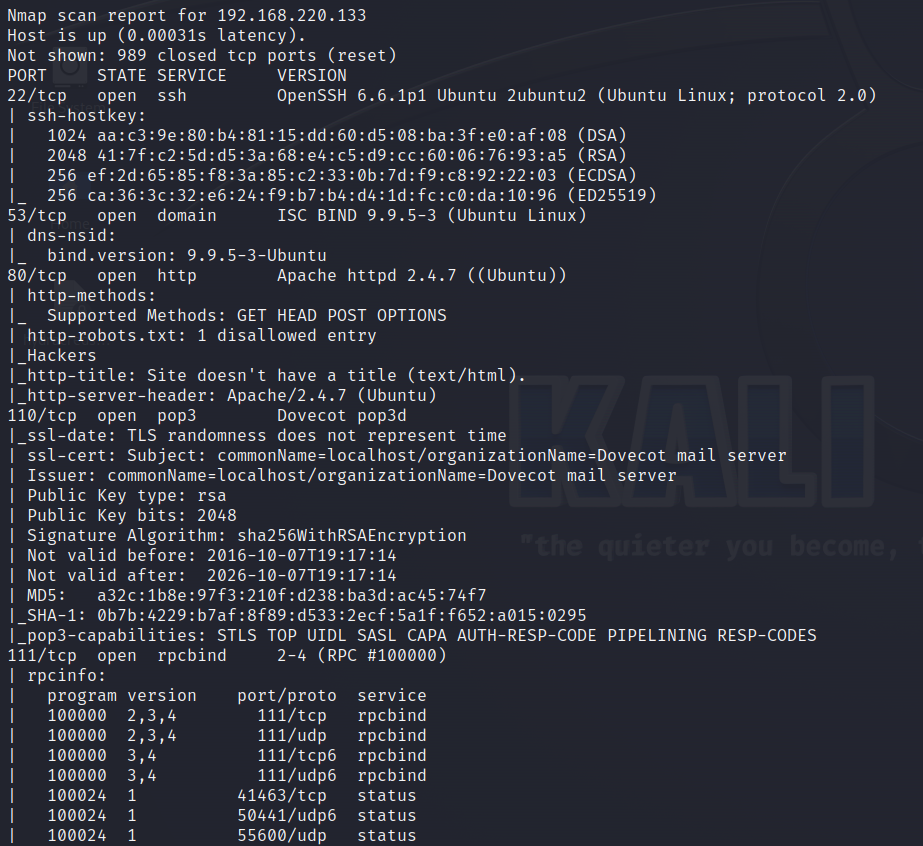
**<**Detail here using sub sections for strengths and weaknesses**>**

# Technical Findings

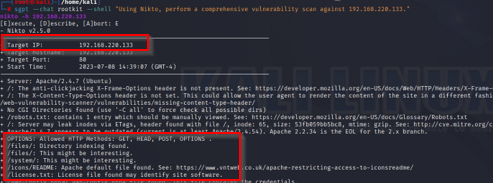
XLSC was able to gain internal network access through the methods provided by the client (VPN) for internal penetration testing purposes. Once a connection was established to the internal client network, XLSC was able to identify several reachable hosts.



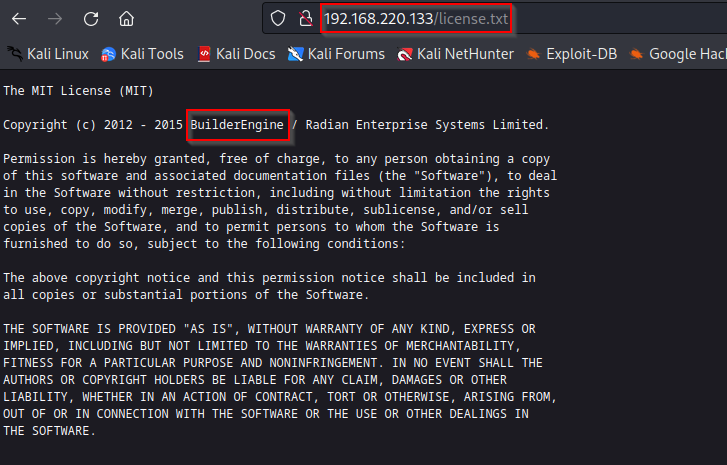
*Fig 1 – Using Nmap the 192.168.220.0/24 network was scanned and 6 hosts provided a response.*

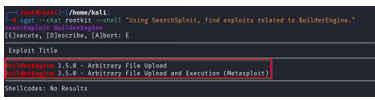


*Figure 3 – Follow up Nmap scans of the 192.168.220.133 device showed an unsecured HTTP port was accessible.*

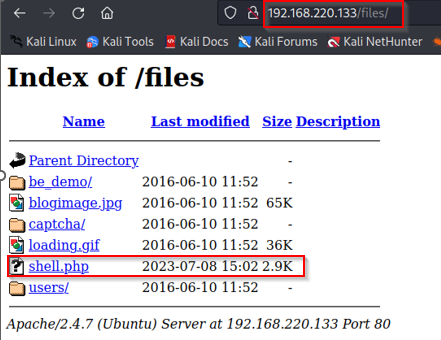


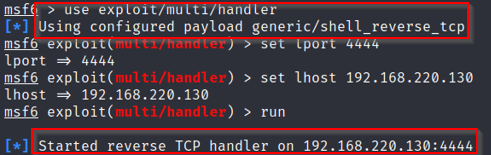
*Figure 3 – Follow up Nikto Vulnerability scans identified a license file for the BuilderEngine Content Management System (CMS).*

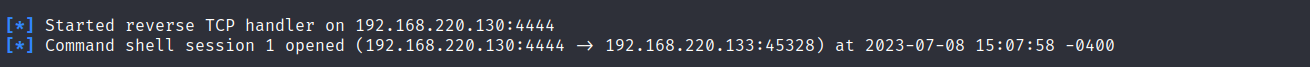


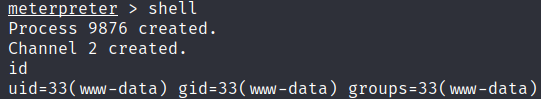


*Figure 4 – Using Searchsploit, a script providing unrestricted file upload for BuilderEngine was located. Modification of the script to execute the payload against 192.168.220.133 was successful and a reverse shell payload titled ‘shell.php’ was uploaded.*

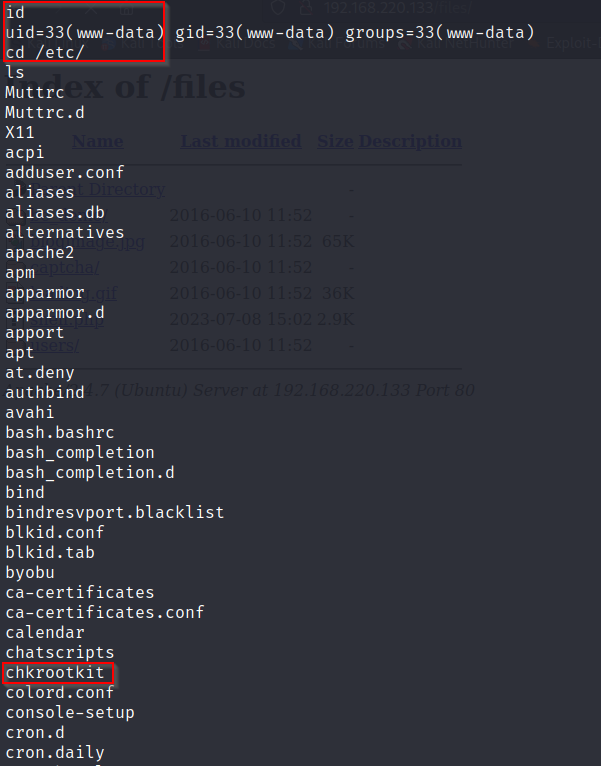




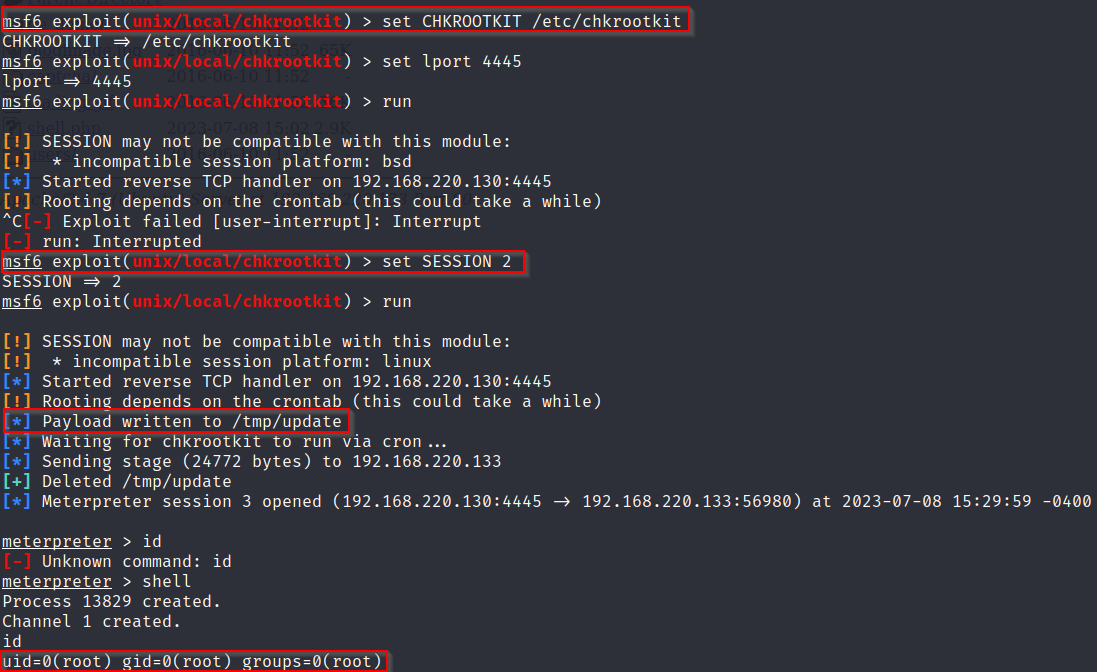




*Figure 5 – Execution of the reverse shell payload from the 192.168.220.133 ‘files’ directory provided initial access with a low level (www-data user) command session being established.*



*Figure 6 – Local enumeration of the 192.168.220.133 target identified vulnerable software ‘chkrootkit’ in the /etc directory.*



*Figure 7 – Using the Metasploit Framework, a local privilege escalation vulnerability applicable to chkrootkit was identified and successfully exploited, granting root level access over the 192.168.220.133 device, leading to domain compromise.*