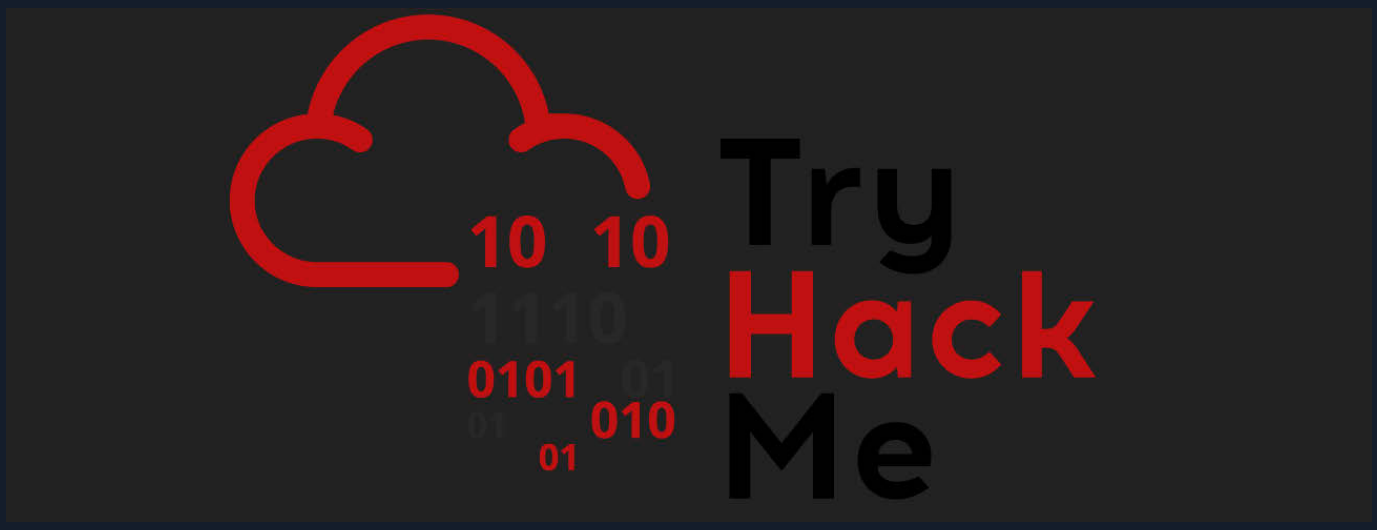


Internal Penetration Test
Report of Findings

Ilya Kravchenko

May 3, 2023

Version 1.0

Table of Contents

Statement of Confidentiality

The contents of this document have been developed by DigiSwit. DigiSwit considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from DigiSwit. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of DigiSwit.

The contents of this document do not constitute legal advice. DigiSwit offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect DigiSwit external or internal infrastructure.

Engagement Contacts

Inlanefreight Contacts		
Primary Contact	**Title**	**Primary Contact Email**
Carlos García Rodriguez	Chief Executive Officer	carlos@digiswit.com

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Ilya Kravchenko	Security Consultant	whereismyfun42@gmail.com

Executive Summary

Daily Bugle ("Daily Bugle" herein) contracted Ilya Kravchenko to perform a Network Penetration Test of Daily Bugle's internally and externally facing network to identify security weaknesses, determine the impact to Daily Bugle, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

Ilya Kravchenko performed testing under a "black box" approach May 3, 2023 without credentials or any advance knowledge of Daily Bugle's internally and externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely via a host that was provisioned specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Ilya Kravchenko sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Ilya Kravchenko were able to gain a foothold in the internal network, Daily Bugle allowed for further testing including lateral movement and horizontal/ vertical privilege escalation to demonstrate the impact of an internal network compromise.

Scope

The scope of this assessment was one internal network range and the Daily Bugle domain.

In-Scope Assets

Host/URL/IP Address	Description
10.10.191.23	Daily Bugle internal network

Table 1: Scope Details

Assessment Overview and Recommendations

During the assessment, the target was compromised using various tools such as Nmap, Gobuster, and John the Ripper. The target was found to be using the Joomla CMS version 3.7.0, and the administrator panel was identified. A cached user password hash was discovered using a Joomla script, and it was later cracked using John the Ripper. This allowed access to the Joomla administrator panel, where a beez3 template was modified to include a reverse shell in PHP. The reverse shell was then used to connect to the target machine. Once on the target machine, it was discovered that the jjameson user had sudo rights to run yum. This vulnerability was exploited using GTFOBins to gain privilege escalation to root.

Recommendations:

1. Upgrade to the latest version of Joomla: Version 3.7.0 of Joomla is outdated and has several known vulnerabilities that can be exploited by attackers. Upgrading to the latest version of Joomla would address these vulnerabilities.

2. Use strong passwords and two-factor authentication: Strong passwords and two-factor authentication can significantly reduce the likelihood of an attacker gaining access to the system.

3. Regularly update and patch software: Regularly updating and patching software can help prevent attacks from exploiting known vulnerabilities.

4. Implement access controls: Restricting user access and privileges can help mitigate the risk of unauthorized access and limit the impact of a successful attack.

5. Regularly conduct security assessments: Conducting regular security assessments can help identify and address vulnerabilities before they can be exploited by attackers.

Network Penetration Test Assessment Summary

Ilya Kravchenko began all testing activities from the perspective of an unauthenticated user on the internal network. Daily Bugle provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

Summary of Findings

During the course of testing, Ilya Kravchenko uncovered a total of seven (5) findings that pose a material risk to Daily Bugle's information systems. Ilya Kravchenko also identified one informational finding that, if addressed, could further strengthen Daily Bugle's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

Finding Severity			
High	**Medium**	**Low**	**Total**
3	**1**	**1**	**5**

Table 2: Severity Summary

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

Finding #	Severity Level	Finding Name
1.	High	Local Administrator Password Re-Use
2.	High	Superuser permissions for binaries enabled
3.	High	Joomla CMS Weak/Default Credentials
4.	Medium	Insecure File Shares
5.	Low	Directory Listing Enabled
6.	Info	Enhance Security Monitoring Capabilities

Table 3: Finding List

Internal Network Compromise Walkthrough

During the course of the assessment Ilya Kravcheno was able gain a foothold and compromise the internal network, leading to full administrative control over the Daily Bugle domain. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to Daily Bugle the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

Detailed Walkthrough

Ilya Kravcheno performed the following to fully compromise the Daily Bugle domain.

1. The tester utilized the nmap and gobuster tool to enumerate the target and obtain possible target directories.
2. The enumeration provided a couple of points of interest: a README file, which disclosed that the target is using the Joomla CMS and its version.
3. The tester then ran the https://github.com/XiphosResearch/exploits/tree/master/Joomblah script which exposed the cached password of the user jonah, his email and password hash.
4. The tester was able to successfully crack this account's password offline by using john the ripper, revealing the clear text value.
5. The tester was able to authenticate to the Joomla CMS and the account happened to be an administrator.
6. This jonah account had administrator rights and is able to redact templates. Which made it possible to rewrite the template at beez3 into a reverse shell.
7. The tester used a netcat listener to receive the reverse shell from the target machine, hence compromising the server and gaining ground as a non-priveleged user.
8. Finally, using the sudo -l command the tester found out, that the yum binary can be used with priveleges and with help of GTFObins a privelege escalation is done..

Detailed reproduction steps for this attack chain are as follows:

Upon connecting to the network, the tester started the nmap and gobuster tools for recon and enumeration.

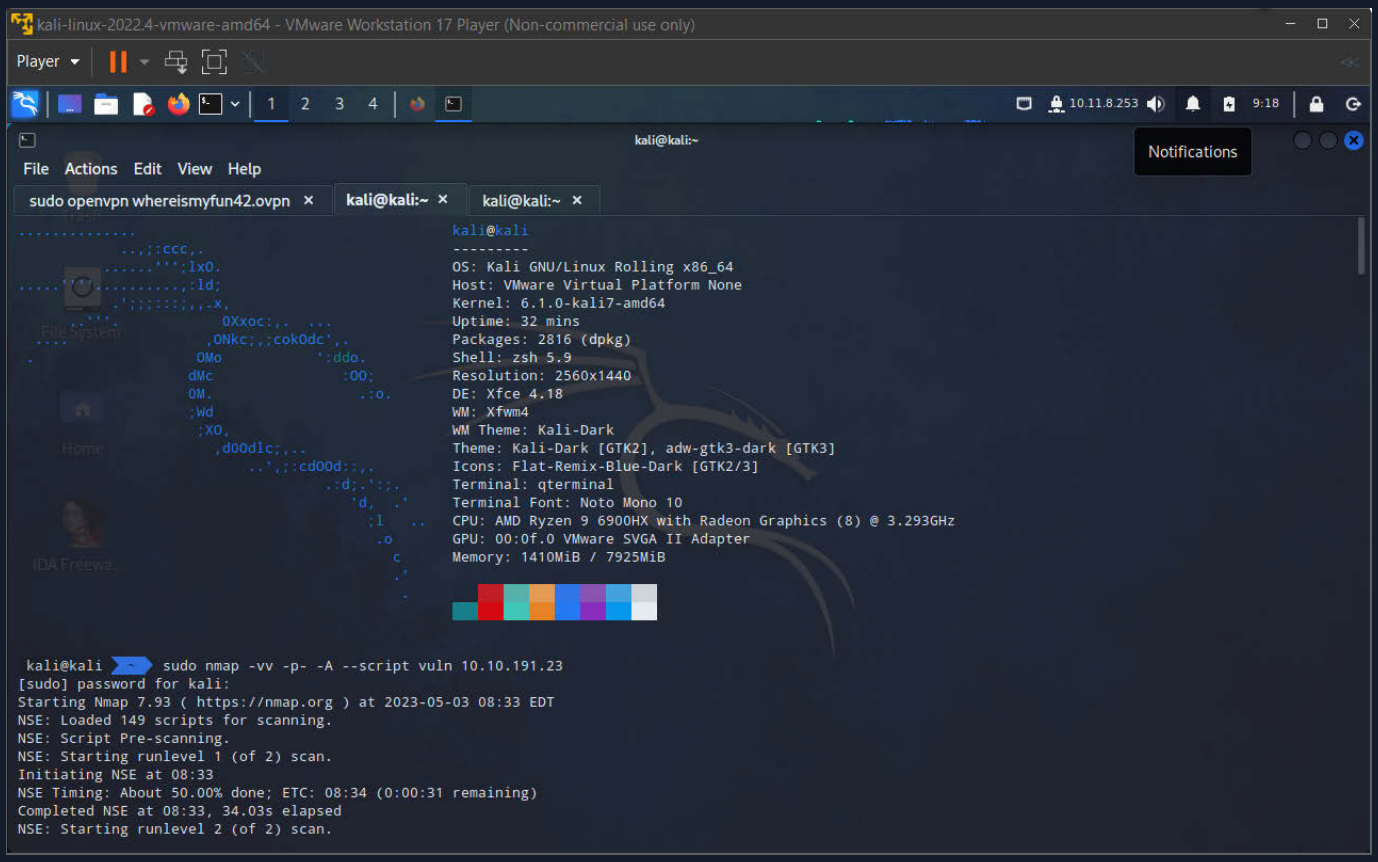
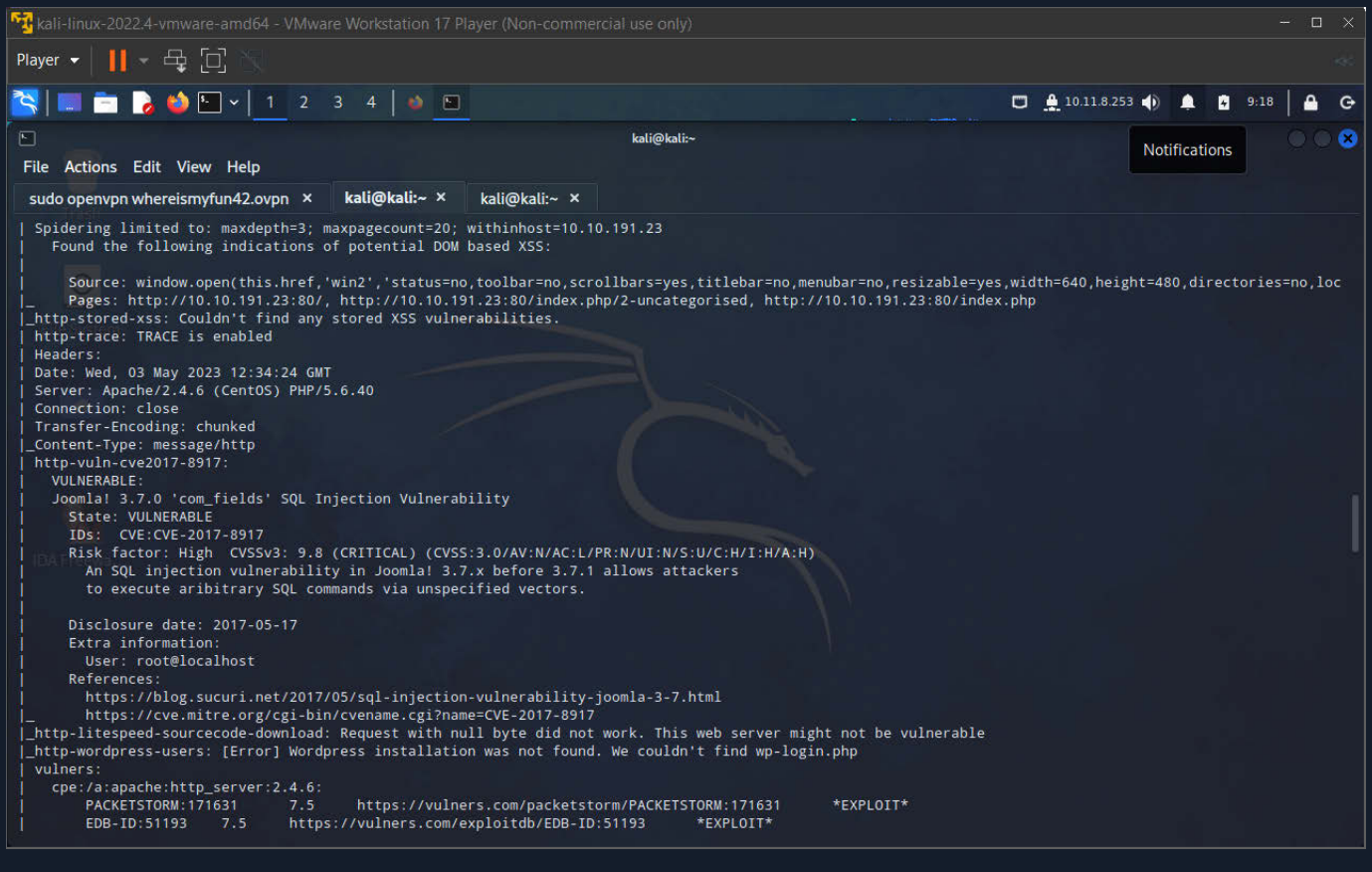
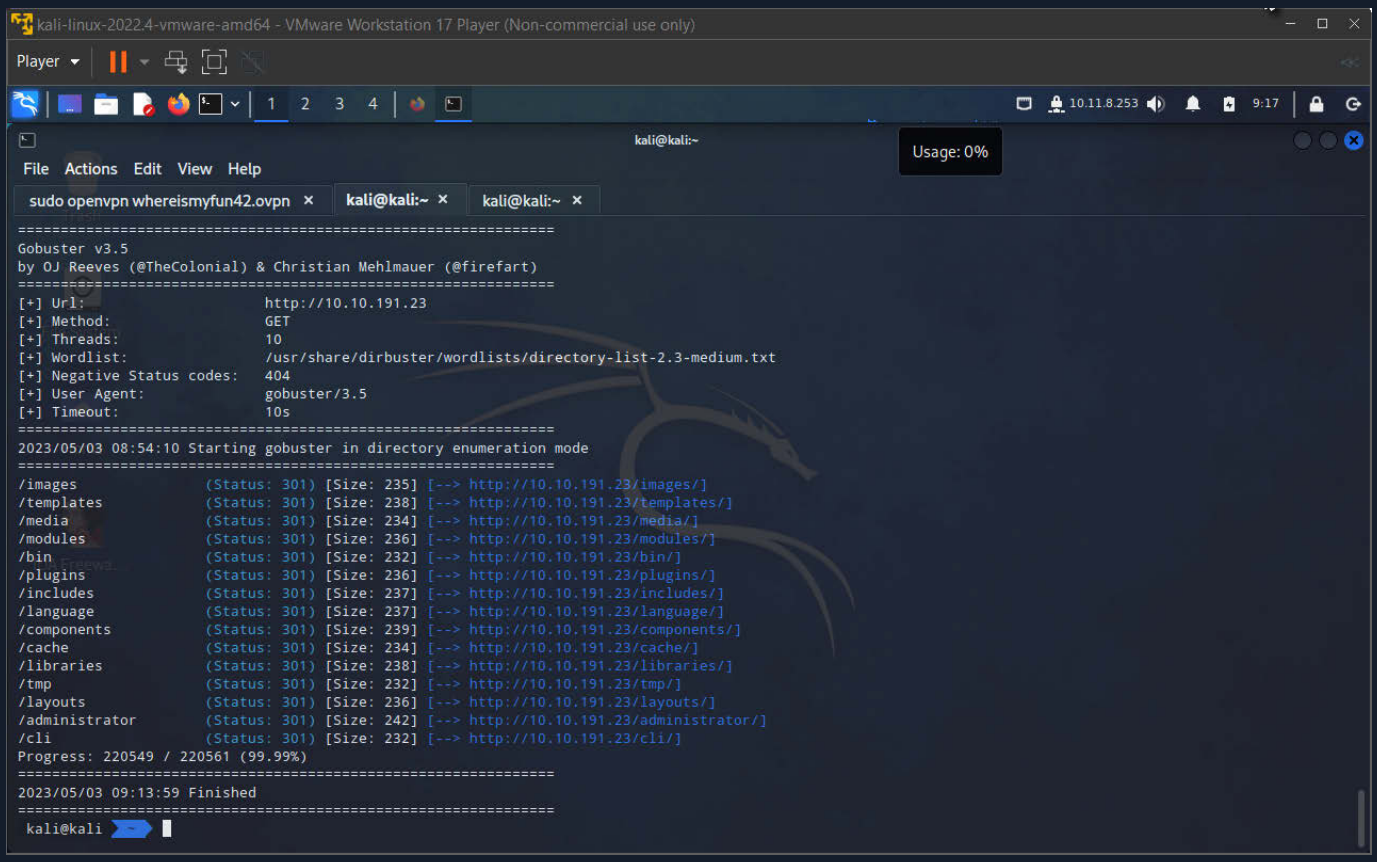
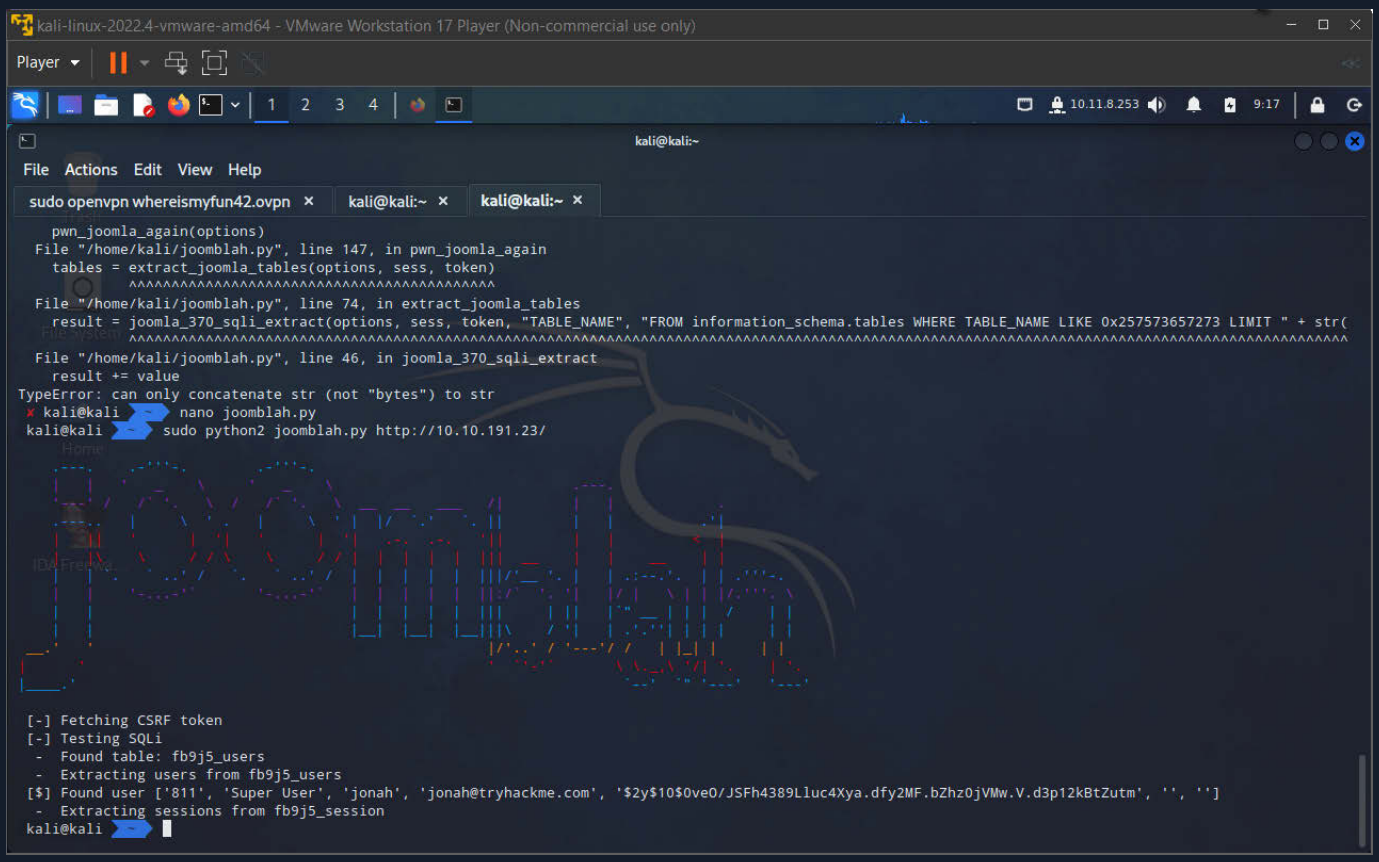


Figure 1: Starting enumeration

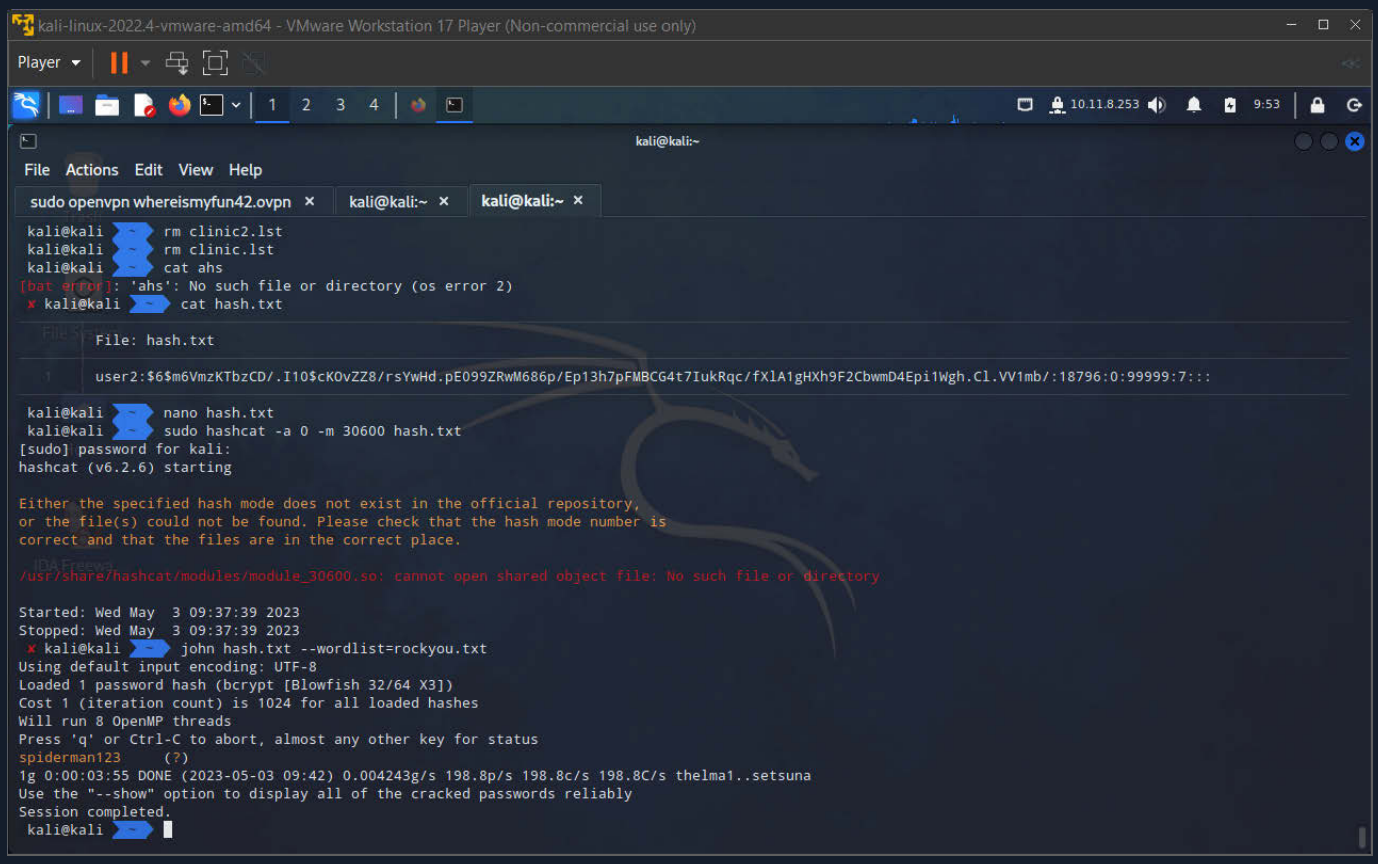




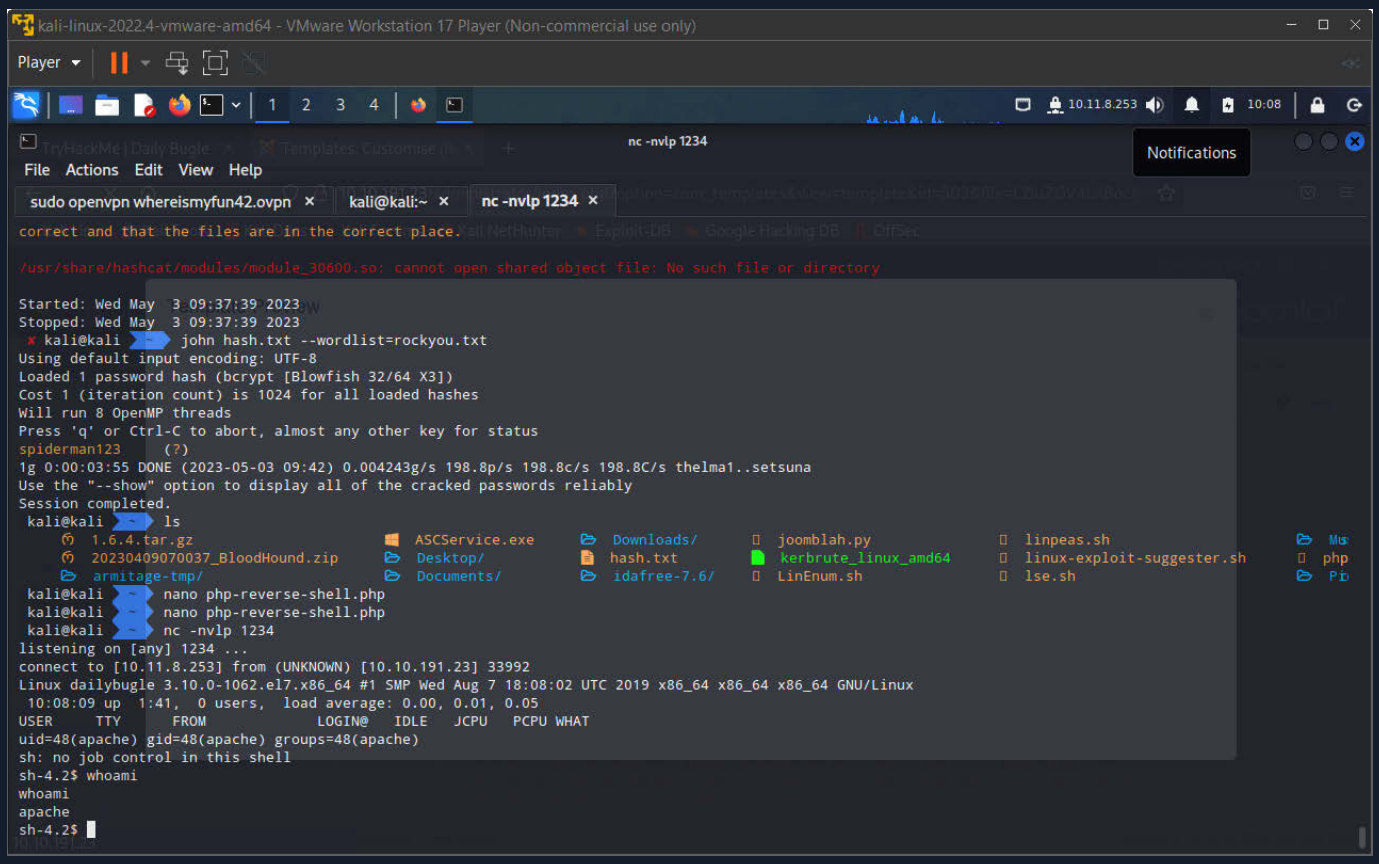
The enumeration exposed some of the endpoints which are of interest - mainly the /administrator and a README file. The README file contains a hint that the server is using a Joomla CMS of version 3.7.0. Which enables a new attack vector - the Joombla python script.



The script showed us cached credentials of a user "jonah" with hased password. To crack the hash John the Ripper is being used.



With a cleartext password we can proceed to the /administrator endpoint, discovered earlier and login into the Joomla CMS with the credentials. As the user has administrator rights, we are able to edit the templates. The beez3 template can be used for that - the index.php is replaced with a reverse php shell from pentestmonkey. After starting a listener with netcat, a shell is received and the server compromised.



Looking through the compromised machine we are able to find out, that yum can be used with sudo rights, which can be exploited. GTFOBins has the needed information on how to gain privelege escalation to a root user, hence fully owning the server.