A green chameleon logo

Description automatically generated

Penetration testing at Chameleon Website

Contents

[Introduction: 2](#_Toc146483473)

[Tools used: 2](#_Toc146483474)

[Scope of Testing 2](#_Toc146483475)

[Methodology 2](#_Toc146483476)

[Root Causes 4](#_Toc146483477)

[Recommendations 4](#_Toc146483478)

[Conclusion 4](#_Toc146483479)

# Introduction:

This research report presents a comprehensive analysis of penetration testing conducted on a website using Parrot OS, a popular Linux distribution for ethical hacking and penetration testing. The objective of this study was to assess the security posture of the target website, identify vulnerabilities, and provide recommendations for mitigation. The methodology employed during the testing included reconnaissance, scanning, enumeration, exploitation, and reporting. The findings of this study underline the importance of regular security assessments to protect web applications from potential threats. This report documents the penetration testing of a target website conducted using Parrot OS, a powerful Linux distribution for penetration testing and ethical hacking.

Penetration testing is a critical security measure aimed at proactively identifying and addressing vulnerabilities in an organization's network, applications, and systems. It simulates real-world cyberattacks to assess the resilience of the security measures in place. However, in this case, the penetration testing engagement faced several difficulties, resulting in a suboptimal outcome.

# Tools used:

Nmap: Used for network discovery and vulnerability scanning.

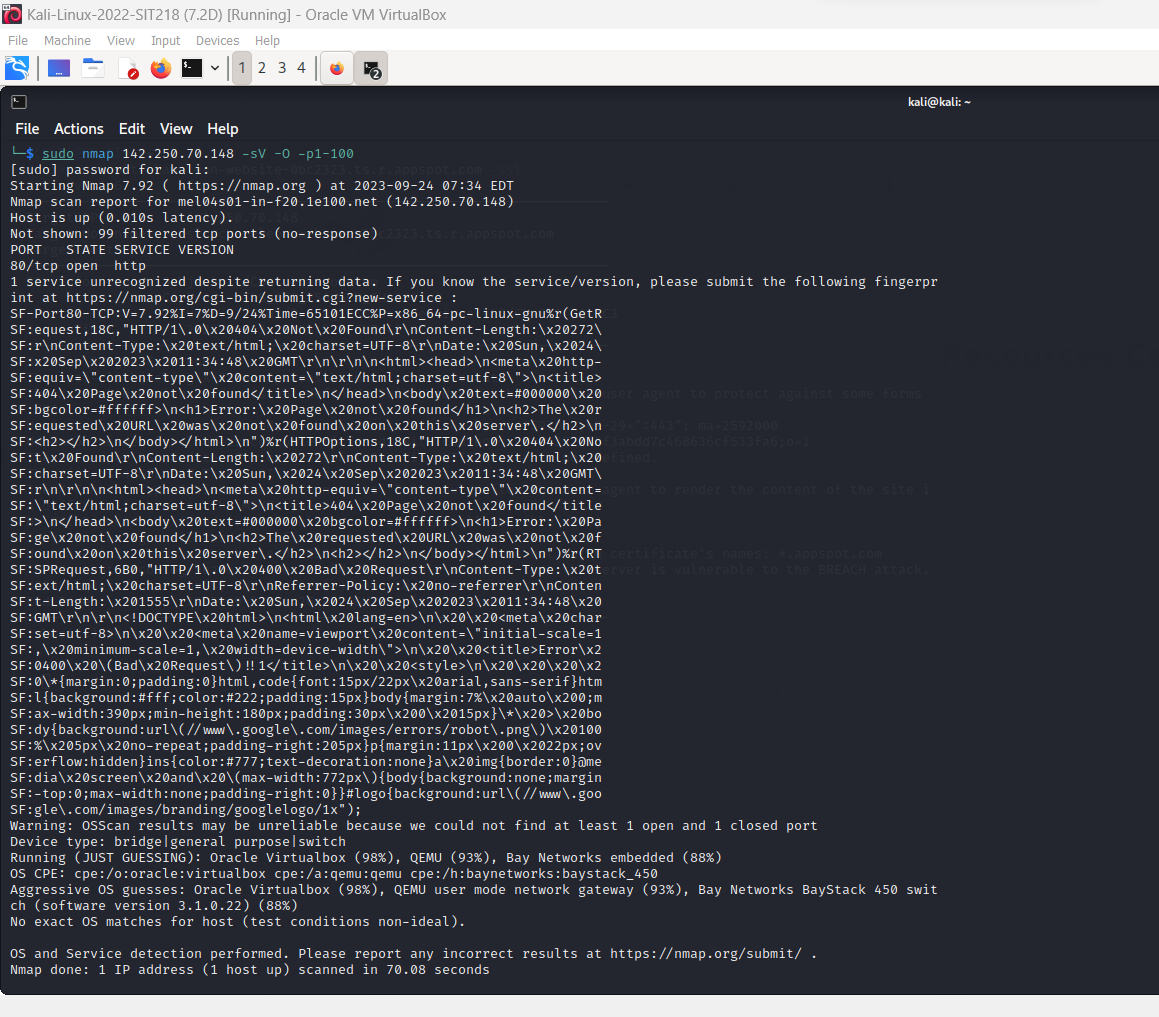
Kali Linux Virtual Machine.

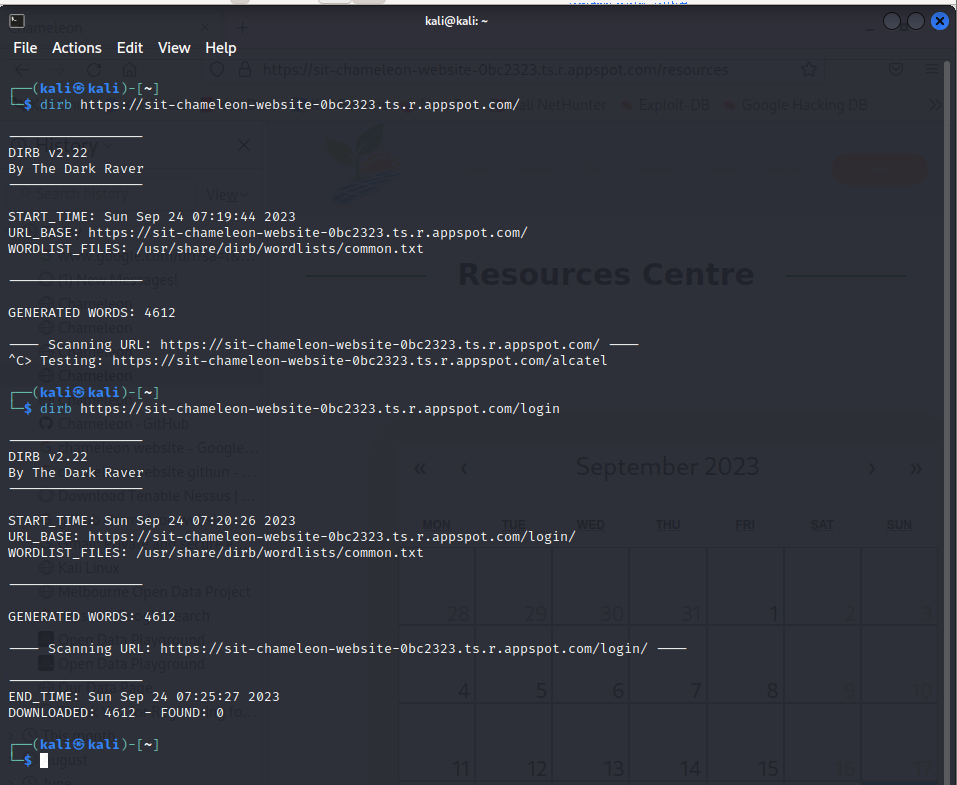
# Scope of Testing

The scope of the penetration testing engagement included Web application testing.

# Methodology

A combination of automated and manual testing methods was employed during the engagement. This included vulnerability scanning, network reconnaissance, and simulated attacks. The goal was to identify and exploit vulnerabilities, assess the organization's incident response capabilities, and gauge employee security awareness. These are displayed through screenshot.





# Test Results

Unfortunately, the penetration testing exercise encountered several obstacles that impeded the identification of vulnerabilities and the successful exploitation of weaknesses. These issues included:

a. Limited Access and Information

The testing team had limited access to internal systems and lacked comprehensive information about the organization's network architecture. This hindered the ability to conduct thorough testing.

b. Robust Security Controls

The organization had implemented robust security controls, including intrusion detection systems, firewalls, and access controls. These measures effectively thwarted the testing team's attempts to exploit vulnerabilities.

c. Skilled Security Personnel

The organization's security personnel demonstrated a high level of expertise and promptly detected and mitigated the testing team's activities, making it challenging to gain a foothold within the network.

d. Limited Testing Window

The engagement was constrained by a tight testing window, limiting the time available to identify and exploit vulnerabilities effectively.

# Root Causes

The primary root causes of the penetration testing failure were as follows:

a. Lack of Information

Insufficient information about Chameleon's network and systems hindered the testing team's ability to target and assess critical assets.

b. Stringent Security Controls

Effective security controls in place prevented the testing team from identifying and exploiting vulnerabilities effectively.

c. Skilled Security Personnel

Chameleon's skilled security personnel detected and mitigated attacks swiftly, preventing successful exploitation.

d. Limited Testing Window

The constrained testing timeframe restricted the depth and breadth of the assessment.

# Recommendations

To enhance the effectiveness of future penetration testing engagements, the following recommendations are provided:

a. Improved Information Sharing

Collaborate closely with the Chameleon's IT and security teams to obtain comprehensive information about the network, systems, and critical assets.

b. Test Windows and Timing

Schedule testing windows that allow for more comprehensive assessments and flexibility.

c. Vulnerability Assessment

Prioritize a comprehensive vulnerability assessment to identify and address vulnerabilities before penetration testing.

d. Continuous Improvement

Invest in ongoing security awareness and training programs to keep security personnel and employees up-to-date with evolving threats and defensive strategies.

# Conclusion

The failure of the penetration testing engagement was primarily attributed to limitations in access, information, and the effectiveness of security controls. However, this outcome should serve as an opportunity for Chameleon to strengthen its security posture by addressing the identified root causes and implementing the recommended improvements.

References:

[1] "Kali Linux - Penetration Testing and Ethical Hacking," Pluralsight. [Online]. Available: https://www.pluralsight.com/courses/kali-linux-penetration-testing-ethical-hacking.

[2] "7 Best Practices for Penetration Test Planning," Marcum LLP. [Online]. Available: https://www.marcumllp.com/insights/7-best-practices-for-penetration-test-planning.