VAPT Report

1. Introduction

Date of Report: September 13, 2024
Target Hostname: 43.205.151.144
Target IP: 43.205.151.144
Scan Performed By: ADSA(Automated Detection and Security Analysis)
Purpose: Identify vulnerabilities and security issues in the target environment.

2. Scan Summary

2.1 Nmap Scan Summary

Scan Start Time: September 13, 2024 16:12:33
Scan End Time: September 13, 2024 16:12:33
Total Ports Scanned: 1000
Open Ports:

Port Id	Service Name
21	ftp
22	ssh
80	http
443	http

Filtered Ports:

Port Id	Service Name
135	msrpc
139	netbios-ssn
445	microsoft-ds
1022	exp2
1023	netvenuechat
1026	LSA-or-nterm
9898	monkeycom

Host Status: up

2.2 Nikto Scan Summary

Scan Start Time: September 13, 2024 16:12:33
Scan End Time: September 13, 2024 16:12:33
Target Port: 80
Server Detected: N/A

3. Vulnerability Assessment

3.2 Filtered Ports

Filtered ports may indicate that they are protected by a firewall or that the service is not responding to probes. These ports might not be directly accessible but should be reviewed for security controls.

3.3 Web Application Security

4. Recommendations

1. Review and Harden MySQL Configuration:
- Secure MySQL service and apply relevant patches.
2. Web Server Configuration:
- Verify the presence and configuration of the web server on port 80.
3. Filter Rules Review:
- Review firewall and security rules for filtered ports to ensure proper protection and accessibility.
4. Regular Updates and Patching:
- Ensure that all services, including MySQL and web servers, are kept up-to-date with the latest security patches.

5. Conclusion

This assessment highlights the key areas where the target system can be improved. Addressing the identified issues will enhance the security posture and reduce potential risks. Regular security assessments and best practices should be followed to maintain a secure environment.

6. Appendices

6.1 Tools Used

- Nmap: Network scanner for identifying open ports and services.
- Nikto: Web server scanner for identifying common vulnerabilities and misconfigurations.

6.2 References

- [Nmap Documentation](https://nmap.org/docs.html)
- [Nikto Documentation](https://cirt.net/Nikto2)