IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 9, April 2025

Impact Factor: 7.67

Metasploit for Exploit Automation and Threat Detection on Linux

Prof. Subhkirti Bodkhe, Prof. Mrunali Jadhav, Sujal Warkar

Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, India

warkarsujal@gmail.com

Abstract: *The continuous evolution of cyber threats has necessitated the use of advanced tools for both offensive and defensive security operations. Metasploit, a widely adopted penetration testing framework, offers comprehensive functionalities for exploit automation and vulnerability assessment. In Linux environments, Metasploit's capabilities extend beyond traditional exploitation, serving as a powerful tool for simulating attacks, automating payload delivery, and contributing to threat detection mechanisms. This research explores the application of Metasploit for automating exploits and detecting potential threats in Linux systems, emphasizing its role in securing enterprise networks and strengthening incident response strategies.*

Keywords: Metasploit Framework, Exploit Automation, Penetration Testing, Threat Detection, Linux Security, Vulnerability Assessment, Intrusion Detection, Offensive Security, Cybersecurity, Incident Response, IDS/IPS Integration, Ethical Hacking, Security Hardening, Linux System Exploitation, CVE Exploitation, Payload Generation, Automated Threat Hunting

DOI: 10.48175/IJARSCT-25775