JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Audit on Security Tools in Kali Linux

Sridevi Ravi, Ishwari Bhor, Mayuri Bapat

Student, Department of Science and Computer Science, (Cyber and Digital Science), MIT college of Arts, Commerce and Science

Authors

Sridevi Ravi

Ishwari Bhor

Mayuri Bapat

Abstract

Kali Linux, is a powerful and open source platform which has various types of tools (arsenal type of tools). These tools are used for various regions to empower cyber security, data integrity, confidentiality etc. This platform is mainly designed for penetration testing for ethical hackers, digital forensics, and for security auditing purposes. The tool kits in kali linux has a vast range of utilities which are specially made for ethical hacking purpose and for security assessment, digital defense purpose.

By this review paper we will get to know a diverse range of security tools in Kali Linux, which include the purpose of the specific tools, the features provided by the tools, And where the tools are implemented in our daily life or for security purposes. We are going to begin this with how do we categorize the security tools in Kali Linux on the basis of reconnaissance, vulnerability, exploitation, privilege escalation, forensics, packet sniffing, pivoting, and many more.

These tools are only used for security reasons only. If any illegal activities occur they may lead to severe consequences. We are going to see a review on notable or widely used tools such as Nmap for network reconnaissance, Metasploit for penetration testing and exploitation, Wireshark for packet analysis, John the ripper for Password cracking and many more. These also evaluates the efficiency, usability, and versatility of these tools, providing many insights on their practical applications and for potential limitations of the tools.

In conclusion, this review paper gives knowledge of and value of Kali Linux tools in different platforms for security professionals, ethical hackers, cyber security analysts. By providing them a wide range of powerful tools and specialized security tools. It empowers users to conduct thorough security assessments, identify different vulnerabilities, and ensures a safe and secure digital infrastructure against evolving threats.

Introduction

Kali Linux, is a Linux distribution which is designed specially for digital forensics, penetration testing and for security assessment. This Kali Linux software is maintained and funded and supported by Offensive Security. Kali Linux software is based on the **Debian** testing branch and it is specially known for robust security-focused features. It offers a rich ecosystem of pre-installed tools for conducting penetration testing, vulnerabilities assessment or for digital forensics purposes. The Kali Linux users should be familiar with the most used or top most used ones such as Nmap, Metasploit, John the ripper, Wireshark, Burp Suite, Hydra, Maltego, Nessus, Skip fish, Bloodhound, Hash cat, Aircrack, Lynis, Autopsy, Sqlmap, Netcat, WPScan, SlowHTTPTest, t50, and nikto. These tools play a crucial role for assessing vulnerabilities, ensuring for safe and secure system security, Data integrity, and Ensuring a great and powerful defense against various cyber threats evolving in this digital era. Ensuring a safe and secure system or Network Communications, Transactions, Data Confidentiality, Tampering or manipulation of Confidential Messages, or for digital forensics. Let us get a knowledge about These tools:

Nmap (Network Mapper): Nmap is a powerful open source tool which is used to scan for networks, open ports, etc.

Purpose of Nmap tool Network Discovery, Security auditing, Network Inventory, Port Scanning.

Features of Nmap which are very useful such as InBuilt Port Scanning Technique, Operating System Detection, Service version Detection, Scriptable Interaction, Host Discovery, Output Flexibility(Outputs like Normal text, XML, etc), and Flexible Target Specification(It targets on specific hosts by using IP Address, IP names, and Host names etc.

Uses of Nmap tool: Nmap tool mainly Focuses on Network Security Auditing(It is useful for organizations to identify open ports and potential vulnerabilities and Secure them by resolving vulnerabilities), Penetration testing (ethical hackers and security professionals use nmap during penetration testing for open ports and many other vulnerabilities for further exploitation), Network Troubleshooting, Compliance audits(to ensure network security requirements in Payment card Industry Data Security Standard),and Asset Management.

Metasploit: Metasploit is used for penetration testing for security professionals and ethical hackers to identify potential risks and exploit using potential risks and validate the vulnerabilities in our computer systems. It offers a wide range and suite of tools for penetration testing and vulnerability assessment and for exploit development.

Purpose penetration testing, exploit development, vulnerability validation, security research, education and training

Features of Metasploit: Exploit Modules, Payloads, Auxiliary Modules, Post-Exploitation Modules, Exploit Development Tools, Integration with Other Tools

Uses of Metasploit: Penetration Testing, Vulnerability Assessment, Red Team Operations, Incident Response, Security Research

John The Ripper: John the Ripper is a widely used tool and it is a popular tool for powerfully cracking passwords which is used primarily for recovering passwords from hashed formats. And it is widely used by security professionals, ethical hackers, and system administrators to strengthen their passwords and to find an effective mechanism for password storage.

Purpose of John The Ripper: Password Cracking, Password Auditing, Password Recovery

Features of John The Ripper: Multiple Attack Modes, Customizable Rules, Hash Types, Performance Optimization, Incremental Mode

Uses of John The Ripper: Security Assessments, Password Recovery, Forensic Analysis, Password Policy Enforcement, Research and Development.

Wireshark: Wireshark is a widely used tool for network protocol analyzer. This allows users to capture the browser traffic running on the computer and it is used for network troubleshooting analysis and security and protocol development and for education purposes.

Purpose of Wireshark: Network Traffic Analysis, Network Troubleshooting, Security Analysis

Features of Wireshark: Packet Capture, Protocol Support, Packet Filtering and Display Filters, Packet Decoding, Graphical Analysis Tools, VoIP Analysis, Export and Reporting

Uses of Wireshark: Network Troubleshooting, Security Monitoring, Protocol Development, Network Forensics, Educational Purposes

Burp Suite: Burp Suite is a widely used set of tools which are powerful and designed for web application security testing. It is used by security professionals, ethical hackers, and developers for identifying vulnerabilities and to access the security of web applications.

Purpose of Burp Suite:Web Application Security Testing, Vulnerability Assessment, Security Research

Features of Burp Suite:Proxy, Scanner, Spider, Repeater, Intruder, Scanner Extensions

Uses of Burp Suite: Penetration Testing, Secure Development, Security Training, Incident Response, Compliance Audits.

Hydra: Hydra is a popular and powerful password-cracking tool that is used to perform brute-force attacks and dictionary attacks against various network services. It is commonly used by security professionals, penetration testers, and ethical hackers to assess the security of authentication mechanisms and recover passwords from protected resources.

Purpose of Hydra:Password Cracking, Network Security Assessment

Features of Hydra**:** Support for Multiple Protocols,Brute-Force and Dictionary Attacks, Parallel and Distributed Processing, Customizable Parameters, Session Management

Use of Hydra: Penetration Testing, Password Recovery, Network Forensics, Educational Purposes

Maltego: Maltego is a powerful data visualization and link analysis tool used for gathering and analyzing information about individuals, organizations, and networks. It is commonly utilized in various fields such as cybersecurity, law enforcement, intelligence gathering, and fraud detection.

Purpose of Maltego: Data Visualization and Link Analysis, Open-Source Intelligence (OSINT), Threat Intelligence

Features of Maltego: Graph-Based Data Visualization, Entity Transformations, Integration with Data Sources, Link Analysis and Pattern Recognition, Collaboration and Sharing

Uses of Maltego: Cybersecurity Investigations, Fraud Detection and Financial Investigations, OSINT Research, Business Intelligence and Competitive Analysis, Digital Marketing and Brand Monitoring.

Nessus: Nessus is a powerful tool which is widely used by IT professionals, security professionals, system administrators, and ethical hackers to access the security in their IT environments for identifying security vulnerabilities and to remediate it within their network applications or in the systems.

Purpose of Nessus: Vulnerability Detection, Security Compliance, Risk Assessment

Features of Nessus: Vulnerability Scanning, Plugin Architecture, Customizable Scanning Policies, Asset Discovery, Remediation Guidance, and Integration with SIEM and Ticketing Systems.

Uses of Nessus: Regular Vulnerability Assessments, Compliance Audits, Incident Response, Patch Management, and Risk Management.

Skipfish: Skipfish is an open-source web application security scanner designed to identify security vulnerabilities in web applications. It is widely used by security professionals, penetration testers, and developers to assess the security posture of web applications and identify potential vulnerabilities that could be exploited by attackers.

Purpose of Skipfish: Web Application Security Testing, Vulnerability Assessment

Features of Skipfish: Fast and Scalable, Comprehensive Security Checks, High Accuracy, Customizable Scan Configuration, Reporting

Use of Skipfish: Web Application Security Testing, Secure Development Lifecycle, Compliance Audits, Incident Response

BloodHound: BloodHound is a powerful and popular open-source tool used for Active Directory (AD) domain privilege escalation, reconnaissance, and attack path analysis. It is commonly used by security professionals, penetration testers, and red teams to identify and exploit vulnerabilities in Active Directory environments.

Purpose of BloodHound: Active Directory Reconnaissance, Attack Path Analysis

Features of BloodHound: Graphical Interface, Data Collection, Attack Path Calculation, Visual Analytics, Automated Queries and Calculations, Reporting

Uses of BloodHound: Active Directory Security Assessments, Privilege Escalation Testing, Incident Response, Security Awareness Training

Hashcat: Hashcat is a powerful open-source password recovery tool used for recovering lost or forgotten passwords from various types of hashed data. It supports a wide range of hashing algorithms and attack modes, making it a versatile tool for security professionals, penetration testers, and researchers.

Purpose of Hashcat: Password Cracking

Features of Hashcat: Wide Range of Hashing Algorithms, Multiple Attack Modes, GPU Acceleration, Optimized Performance, Customizable Attack Parameters, Session Management

Uses of Hashcat: Password Recovery, Penetration Testing, Forensic Analysis, Research and Development.

Aircrack-ng: Aircrack-ng is a powerful set of tools which are used for testing the security of wireless networks.

Purpose of Aircrack-ng: Wireless Network Security Assessment

Features of Aircrack-ng: Packet Capture, Packet Injection, Cracking Encryption Keys, Attack Modes, Offline Cracking, Integration with Other Tools

Uses of Aircrack-ng: Wireless Security Audits, Penetration Testing, Forensic Analysis, Security Research and Education.

Lynis: Lynis is an open-source security auditing tool designed for Unix and Linux-based systems. It helps system administrators, security professionals, and auditors assess the security configuration of their systems, identify vulnerabilities, and implement best security practices.

Purpose of Lynis: Security Auditing

Features of Lynis: System and Configuration Checks, Vulnerability Assessment, Compliance Auditing, Reporting and Recommendations, Customizable Scanning, Integration with Security Tools

Uses of Lynis: System Hardening, Security Assessments, Compliance Audits, Security Monitoring, Incident Response.

Autopsy: Autopsy is an open-source digital forensics platform used for analyzing and investigating digital evidence from computers, smartphones, and other digital devices. It is widely used by law enforcement agencies, forensic examiners, and incident response teams to collect, analyze, and report on digital evidence in criminal investigations, civil litigation, and cybersecurity incidents.

Purpose of Autopsy: Digital Forensics Analysis

Features of Autopsy: Disk Imaging and Analysis, File Recovery and Carving, Keyword Search and Indexing, Timeline Analysis, Artifact Analysis, Reporting and Documentation.

Uses of Autopsy: Criminal Investigations, Civil Litigation, Incident Response, Digital Forensics Training, Corporate Investigations.

SQLMap: SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. SQL injection is a common attack vector that allows attackers to manipulate SQL queries executed by a web application's backend database.

Purpose of SQLMap: SQL Injection Testing

Features of SQLMap: Automated SQL Injection Detection, Database Fingerprinting, Enumeration of Database Schema and Data, Exploitation of SQL Injection Vulnerabilities, Post-exploitation Activities, Customization and Configuration

Uses of SQLMap: Penetration Testing, Web Application Security Audits, Bug Bounty Programs, Security Training and Education, Incident Respons.

Netcat: Netcat, often abbreviated as nc, is a versatile networking utility used for reading from and writing to network connections. Originally developed for Unix-like operating systems, Netcat has become a standard tool in network diagnostics and troubleshooting, as well as a component of various security tools and penetration testing frameworks.

Purpose of Netcat: Network Communication

Features of Netcat: Port Scanning, File Transfer, Remote Shell Access, Banner Grabbing, Proxying, Port Forwarding

Uses of Netcat: Network Diagnostics, Penetration Testing, File Transfer, Remote Administration, Security Monitoring

WPScan: WPScan is a widely-used open-source security scanner specifically designed for WordPress websites. It helps in identifying security vulnerabilities, misconfigurations, and weaknesses within WordPress installations. Below are the purpose, features, and common use cases of WPScan:

Purpose of WPScan: WordPress Security Assessment

Features of WPScan: Vulnerability Scanning, Enumeration of WordPress Installations, Brute Force Attack Detection, User Enumeration, Plugin and Theme Enumeration, Configuration Assessment, Reporting and Documentation

Uses of WPScan: Website Security Audits, Penetration Testing, Continuous Security Monitoring, Security Research and Education, Incident Response

SlowHTTPTest: SlowHTTPTest is a command-line security testing tool designed to simulate slow HTTP denial-of-service (DoS) attacks against web servers. It helps security professionals, penetration testers, and system administrators assess the resilience of web servers against slow HTTP-based attacks.

Purpose of SlowHTTPTest: Denial-of-Service Testing

Features of SlowHTTPTest: Slow Request Simulation, Customizable Request Parameters, Support for Various HTTP Methods, Connection Reuse and Recycling, Verbose Output and Logging.

Uses of SlowHTTPTest: Denial-of-Service Resilience Testing, Penetration Testing, Incident Response Preparation, Security Research and Education, Compliance Audits.

T50: T50 is a specialized network stress testing tool designed to generate high volumes of network traffic to test the resilience and performance of network devices, such as firewalls, routers, and intrusion detection/prevention systems.

Purpose of T50: Network Stress Testing

Features of T50: Traffic Generation, Customizable Attack Parameters, Fuzzing Support, Bandwidth Saturation,Performance Benchmarking, Distributed Attack Support

Uses of T50: Network Device Testing, Intrusion Detection System (IDS) Testing, Denial-of-Service (DoS) Testing, Performance Optimization, Training and Education

Nikto: Nikto is an open-source web server scanner designed to perform comprehensive security assessments of web servers and web applications. It helps security professionals, penetration testers, and system administrators identify security vulnerabilities, misconfigurations, and weaknesses in web servers and web applications.

Purpose of Nikto: Web Server and Web Application Security Assessment

Features of Nikto: Vulnerability Scanning, Web Server and Web Application Enumeration, Common CGI Vulnerability Checks, SSL/TLS Security Checks, Directory and File Enumeration, Customizable Scan Options, Reporting and Documentation

Uses of Nikto: Web Server Security Audit, Penetration Testing, Incident Response, Preparation, Compliance Audits, Security Research and Education

Conclusion: In this review paper, we've learned and understand the functionality, significance, and responsible usage of these essential tools. Remember to use them ethically and with proper authorization. Kali Linux remains an indispensable resource for cyber security professionals worldwide. Instead of using separate tools for different reasons, Kali Linux one operating system supports all those tools. There are many tools included in this operating system called Kali Linux but in this review paper we have discussed only the top most important 20 tools which are very useful and powerful and highly used tools. Overall we have to use these tools in an ethical way only, otherwise there are severe consequences. Kali Linux provides a rich ecosystem of security tools, and this review highlights ten essential ones.

References: 1)21 Best Kali Linux Tools for Hacking and Penetration Testing (itsfoss.com) 2) Top 19 Kali Linux tools for vulnerability assessments | Infosec (infosecinstitute.com) 3) 15 Best Kali Linux Tools: A Developer's Guide to Security (theknowledgeacademy.com) 4) Hardening Kali Linux - Kali Linux security (linuxconfig.org)
5) The Top Eight Kali Linux Tools [2024] (simplilearn.com)
6) Top 10 Kali Linux Tools For Hacking - GeeksforGeeks
7) 25 Best Kali Linux Tools (phoenixnap.com)
8) Kali Linux - Wikipedia