Penetration Testing and Log Analysis Dashboard: ReconX

1. Introduction

In the evolving landscape of cybersecurity, efficient penetration testing and log analysis play a crucial role in identifying vulnerabilities and mitigating threats. The **ReconX** dashboard is an automated security toolkit that integrates multiple security scripts, enabling penetration testers and system administrators to streamline network assessments. This report follows the **STAR (Situation, Task, Action, Result) methodology** to document the development and functionality of ReconX.

2. Situation

Organizations face increasing cybersecurity threats, including system vulnerabilities, misconfigurations, and log anomalies that can lead to security breaches. Manual testing and analysis require expertise and can be time-consuming. There was a need for a **centralized and automated** approach that combines multiple security assessment techniques, making it easier for professionals to conduct **port scanning, vulnerability assessments, and log analysis** efficiently.

3. Task

The objective was to develop a command-line dashboard named **ReconX** that would:

- Provide an intuitive interface similar to **Metasploit's msfconsole** for ease of use.
- Run security assessment scripts, including:
  - **Python Log Analysis Script** – To analyze system logs for anomalies.
  - **Bash Vulnerability Analysis Script** – To check for common vulnerabilities on the system.
  - **Remote Vulnerability Analysis Script** – To conduct remote security assessments.
- Automate the execution of these scripts based on user selection.
- Present results in a structured manner for quick interpretation.

4. Action

The development of **ReconX** followed a structured approach:

A. Dashboard Interface Design:

- Created an ASCII-art-based interface similar to Metasploit.
- Implemented a color-coded menu for easy navigation.
- Designed an interactive selection system allowing users to execute different scripts seamlessly.

B. Implementation of Security Scripts:

- Log Analysis (Python): Developed a Python script to parse system logs and detect security anomalies.
- Local Vulnerability Analysis (Bash): Created a Bash script to check for known vulnerabilities in system configurations.
- Remote Vulnerability Analysis: Implemented a script to scan external systems for weaknesses.

C. Automation & Integration:

- Integrated the scripts into the ReconX dashboard for seamless execution.
- Included error handling and output formatting for clarity.
- Provided an option to generate structured reports for further analysis.

D. Testing & Refinement:

- Conducted multiple test runs to ensure the accuracy of results.
- Optimized performance and improved the user experience based on testing feedback.

5. Result

The implementation of **ReconX** successfully addressed the initial cybersecurity challenges by providing:

- A **user-friendly, automated dashboard** for security assessments.
- An efficient **log analysis mechanism** that detects anomalies in system logs.
- A reliable **vulnerability scanning system** that identifies potential security risks.
- A **modular architecture** allowing for future enhancements and additional security tools.

Organizations and cybersecurity professionals can now leverage **ReconX** for quick and effective security assessments, reducing manual effort and improving threat detection capabilities.

6. Conclusion and Future Enhancements

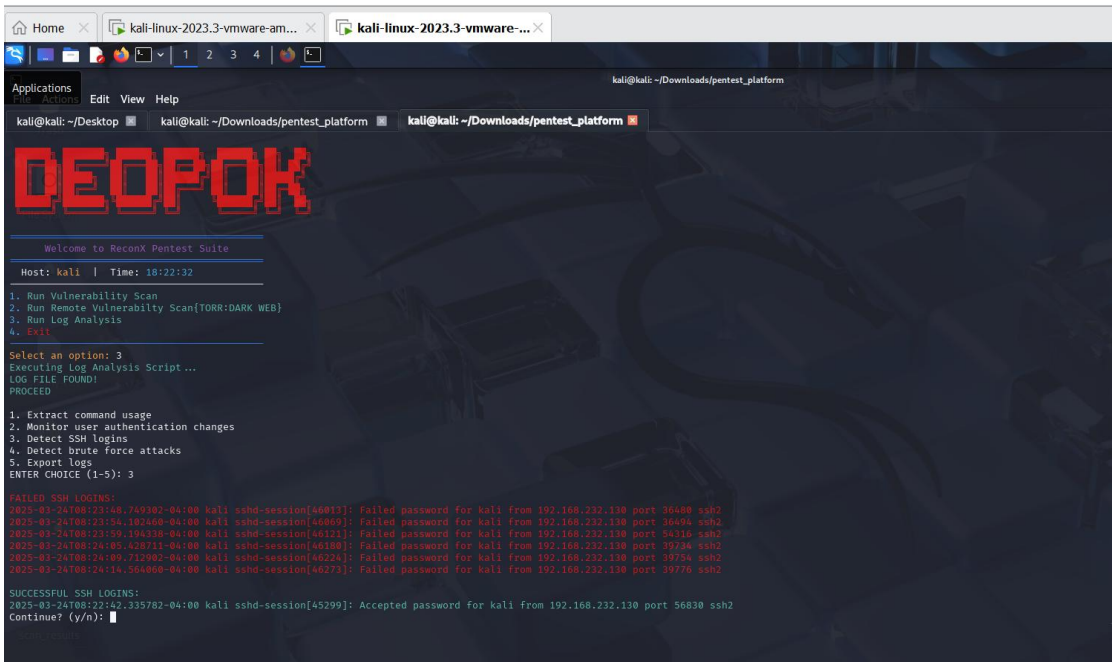
The **ReconX** dashboard successfully integrates penetration testing and log analysis into a single automated platform. Future improvements may include:

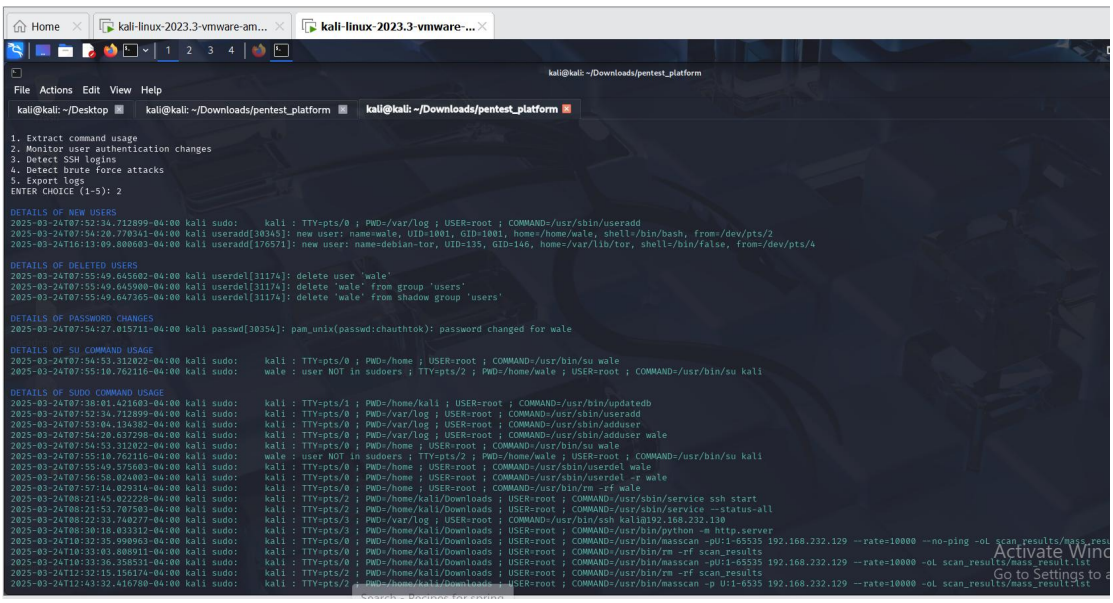
- **Enhanced reporting with graphical visualization.**
- **Integration with external threat intelligence sources.**
- **Support for additional security tools and plugins.**

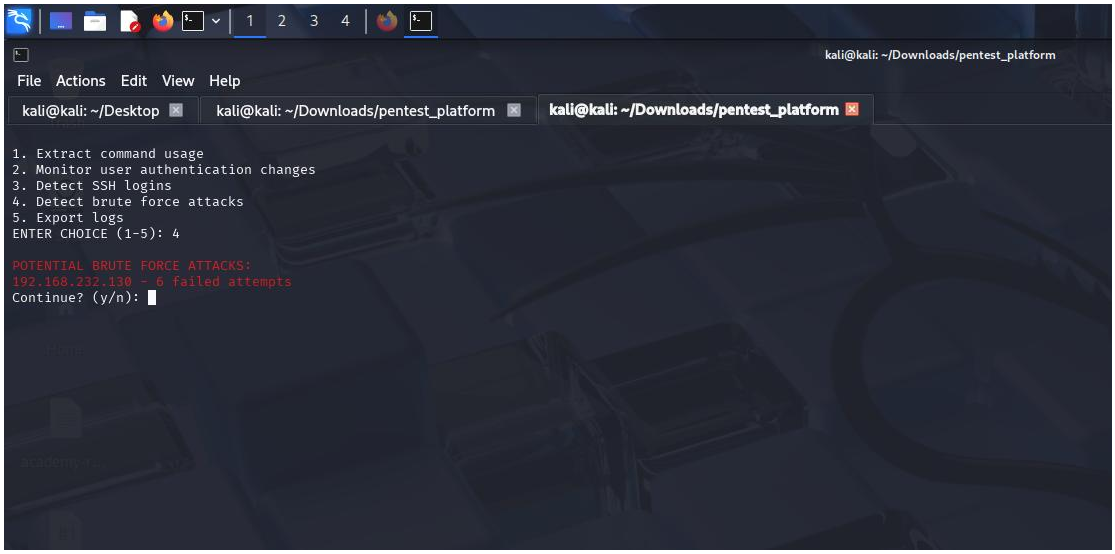
This report serves as documentation for the **design, implementation, and impact of ReconX**. Screenshots showcasing the interface and test results are included in the following section.

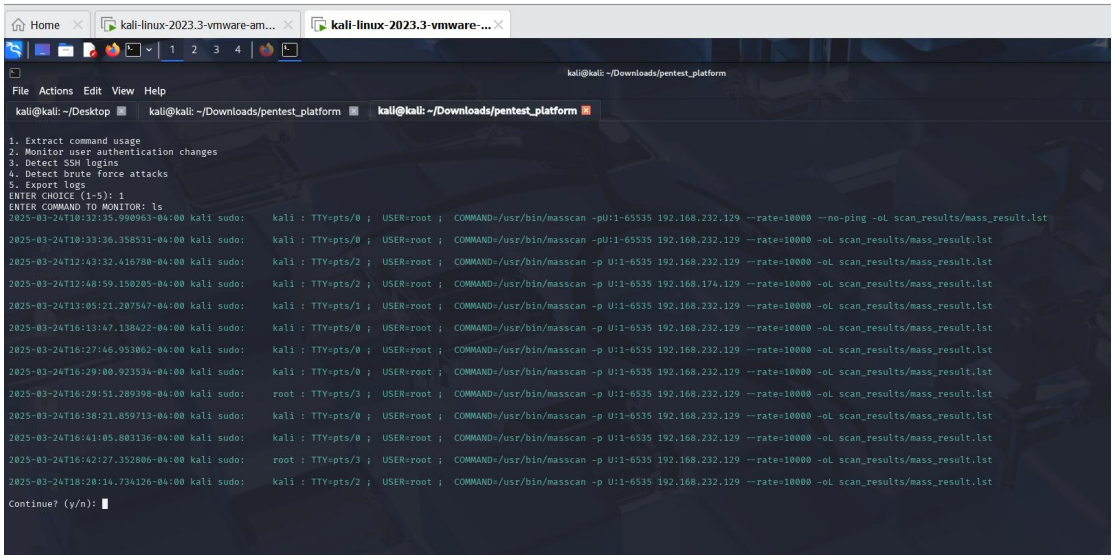
7. Screenshots & Execution Results

LOG ANALYSIS SCRIPT

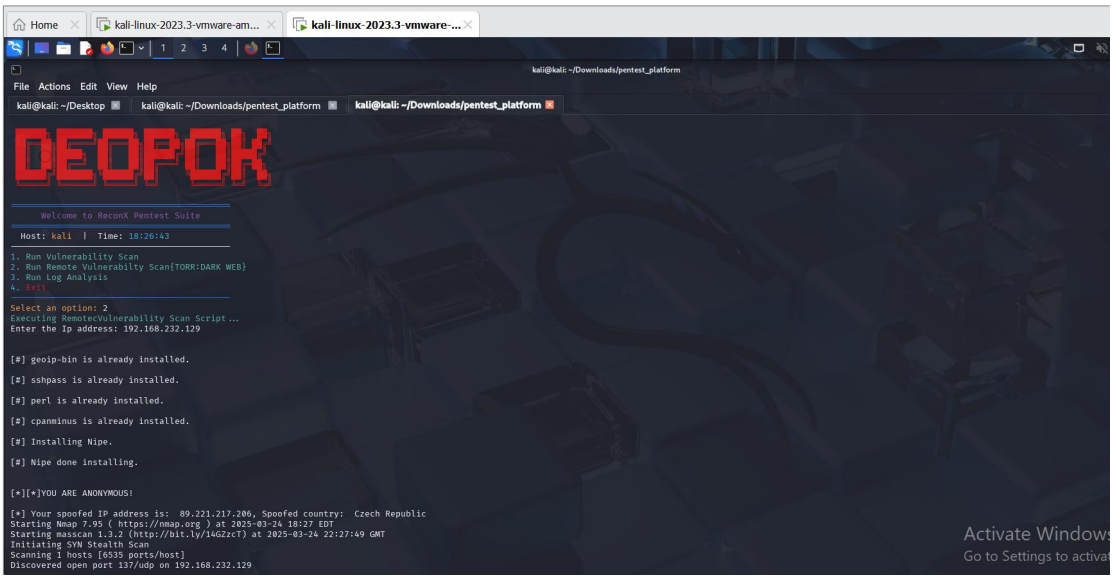





kali@kali: ~/Downloads/pentest_platform
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Downloads/pentest_platform
kali@kali: ~/Downloads/pentest_platform
1. Extract command usage
2. Monitor user authentication changes
3. Detect SSH logins
4. Detect brute force attacks
5. Export logs
ENTER CHOICE (1-5): 4
POTENTIAL BRUTE FORCE ATTACKS:
192.168.232.130 - 6 failed attempts
Continue? (y/n):


Home
kali-linux-2023.3-vmware-am...
kali-linux-2023.3-vmware-...
kali@kali: ~/Downloads/pentest_platform
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Downloads/pentest_platform
kali@kali: ~/Downloads/pentest_platform
1. Extract command usage
2. Monitor user authentication changes
3. Detect SSH logins
4. Detect brute force attacks
5. Export logs
ENTER CHOICE (1-5): 1
ENTER COMMAND TO MONITOR: ls
2025-03-24T10:32:35.990963-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -pU:1-65535 192.168.232.129 --rate=10000 --no-ping -oL scan_results/mass_result.lst
2025-03-24T10:33:36.358531-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -pU:1-65535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T12:43:32.416780-04:00 kali sudo: kali : TTY=pts/2 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T12:48:59.150205-04:00 kali sudo: kali : TTY=pts/2 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.174.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T13:05:21.207547-04:00 kali sudo: kali : TTY=pts/1 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:13:47.138422-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:27:46.953062-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:29:00.923534-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:29:51.289398-04:00 kali sudo: root : TTY=pts/3 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:38:21.859713-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:41:05.803136-04:00 kali sudo: kali : TTY=pts/0 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T16:42:27.352806-04:00 kali sudo: root : TTY=pts/3 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
2025-03-24T18:20:14.734126-04:00 kali sudo: kali : TTY=pts/2 ; USER=root ; COMMAND=/usr/bin/masscan -p U:1-6535 192.168.232.129 --rate=10000 -oL scan_results/mass_result.lst
Continue? (y/n):

Remote Vulnerability Scan Script:



VULNERABILITY SCAN SCRIPT