International Journal of Synergy in Engineering and Technology
IJSET
Journal homepage: https://tatiuc.edu.my/ijset/index.php/ijset/ e-ISSN: 2735-0622

Development of Raspberry-Pi Kali Linux Kit as Vulnerability Scanner

W. A. A. W. Mohamed*, N. M. A. Mohamad, and A. Nasir

University College TATI, Jalan Panchor, Telok Kalong, 24000 Kemaman, MALAYSIA

*Corresponding author email: ainulalyani@uctati.edu.my

KEYWORDS

Vulnerability Scan
Raspberry Pi
Kali Linux Kit
Nmap

ABSTRACT

The development of the Kali Linux Kit for Vulnerability Scan has been an important topic of interest for researchers and practitioners in the field of cybersecurity. Vulnerability scanning is essential to ensuring the security of an organization's network and systems. Traditionally, vulnerability scanning has relied on desktop computers or servers, which lack portability. This necessity has spurred the creation of mobile vulnerability scanning tools compatible with the Kali Linux Kit. This paper is to utilize the Raspberry Pi as a vulnerability analysis kit enables on-the-go vulnerability scans and assessments. Furthermore, early detection of network vulnerabilities is achievable through this project, offering a cost-effective and efficient means of identifying and mitigating potential security risks. Reports detailing Nmap scan results comparing vulnerability detection between desktop computers and Raspberry Pi implementations have been published.

Received 01 April 2020; Revised 28 August 2024; Accepted 30 September 2024; Published 01 October 2024.

1.0 INTRODUCTION

Cyber security is crucial for businesses, governments, and individuals to safeguard their assets, privacy, and personal information from cyber-attacks. Vulnerability assessment techniques are crucial in ensuring cyber security for businesses, governments, and individuals [1]. Vulnerability assessment techniques enable organizations to identify and mitigate potential security risks and threats using automated scanning tools, manual assessments, and penetration testing. These techniques can help organizations prioritize their security efforts, allocate resources effectively, and reduce the risk of cyber-attacks and potential financial, legal, and reputational harm.

Effective vulnerability assessments involve the use of automated scanning tools, manual assessments, and penetration testing to identify weaknesses in systems, networks, and applications [2]. The results of these assessments enable organizations to take proactive measures to strengthen their security posture, prioritize their security efforts, and allocate resources effectively. By conducting regular vulnerability assessments, organizations can reduce the risk of cyber-attacks and protect themselves against potential financial, legal, and reputational harm.

The vulnerability assessment market size is expected to grow from USD 5.5 billion in 2020 to USD 14.5 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 21.2% during the forecast period

[3]. This growth can be attributed to the increasing demand for vulnerability assessment solutions to protect against sophisticated cyber-attacks and the rising need for compliance with regulatory standards.

A survey found that 94% of respondents reported that vulnerability assessments were "somewhat effective" to "very effective" in reducing their organization's cyber risk [3]. The survey also found that 70% of respondents conduct vulnerability assessments at least once a month, indicating the importance placed on regular vulnerability assessments to maintain effective cybersecurity.

By identifying vulnerabilities and weaknesses in systems, networks, and applications, the propose study can take proactive measures with Kali Linux Kit on-the-go vulnerability scans and assessments.

2.0 LITERATURE REVIEW

The use of Kali Linux in Raspberry Pi has been increasingly popular in recent years, as it provides a powerful and portable platform for penetration testing and vulnerability assessment. The Raspberry Pi is a cost-effective and flexible platform for security professionals and hobbyists to perform penetration testing, and Kali Linux is a popular and comprehensive toolkit for penetration testing.

One advantage of using Kali Linux in Raspberry Pi is its portability, as the Raspberry Pi is a small and lightweight device that can be easily carried around, making it ideal for on-site penetration testing. Kali Linux can be easily installed on Raspberry Pi, and its pre-installed tools and packages can be used for a wide range of security assessments, including network scanning, vulnerability assessment, and penetration testing [5].

Another benefit of using Kali Linux in Raspberry Pi is its cost-effectiveness, as the Raspberry Pi is an affordable device that can be easily configured to perform various security assessments. Using Kali Linux in Raspberry Pi can help organizations to perform security assessments on a budget, without compromising on the quality and effectiveness of the assessment [6].

In recent years, researchers have focused on improving the performance and functionality of the Kali Linux Kit. For example, researchers have developed customized scripts and plugins that allow security professionals to automate certain aspects of the vulnerability scanning process. Other researchers have focused on improving the usability and interface of the Kali Linux Kit, making it easier for non-technical users to conduct vulnerability scans.

Overall, the combination of Kali Linux and Raspberry Pi offers a powerful and cost-effective platform for security professionals and hobbyists to perform various security assessments. With its portability and flexibility, it provides a convenient and efficient way to assess the security of a network or system, making it an increasingly popular choice for security assessments. Table 1 shows a comparison between the regular vulnerability scan using desktop computer versus Raspberry Pi Kali Linux Kit.

Table 1: Comparison Vulnerability scan between using desktop computer and Raspberry-Pi

Aspect	Kali Linux Kit	Desktop Computer
Cost	Low	High
Size and Portability	Small and portable	Large and not portable
Processing power and speed	Limited	High
Storage capacity	Limited	High
Ease of use and setup	Moderate	Easy
Range of vulnerability scanning tools	Limited	Extensive
Network connectivity	Limited	Extensive
Power supply	External power supply needed	Built-in power supply

Using a Raspberry Pi as a vulnerability scan tool can be a cost-effective and versatile solution for detecting security flaws in networks and systems. Table 2 indicates that several studies on how a Raspberry Pi can be used for vulnerability assessment.

Table 2: Related works on Vulnerability Scanning using Raspberry-Pi

Study	Purpose	Tool Used	Key Features
[7]	Security Vulnerability Analysis	Advanced IP Scanner, VNC Viewer, Wireshark, Metasploit, and Ettercap	Proves that IoT devices lack a defense mechanism to identify malicious or virus-infected files, making them vulnerable to various attacks
[8]	Network Security Monitoring	Nmap, OpenVAS	Detection of vulnerabilities such as SQL injection, cross-site scripting, and command injection
[9]	Penetration Testing	Custom tool	Scanning for vulnerabilities such as open ports, weak passwords, and outdated software
[10]	Intrusion Detection	Snort	Detection of network threats and vulnerabilities such as SQL injection, cross-site scripting, and command injection
[11]	Web Application Vulnerability Scanning	Custom web application scanner	Detection of vulnerabilities such as SQL injection, cross-site scripting, and command injection
[12]	Network Security Monitoring	Nmap, OpenVAS	Detection of threats such as SQL injection, cross-site scripting, and directory traversal

In conclusion, these studies demonstrate the potential of a Raspberry Pi as a cost-effective and versatile tool for vulnerability scanning and network security monitoring.

3.0 EXPERIMENTAL PROCEDURE

The goal of this paper is to develop a vulnerability scanning tool that will allow security professionals to scan networks for vulnerabilities on-the-go. The tool is built on top of the Kali Linux operating system and is designed to be lightweight and portable. The Kali Linux Kit includes the vulnerability scanning tool Nmap, which allows security professionals to conduct a thorough network scan.

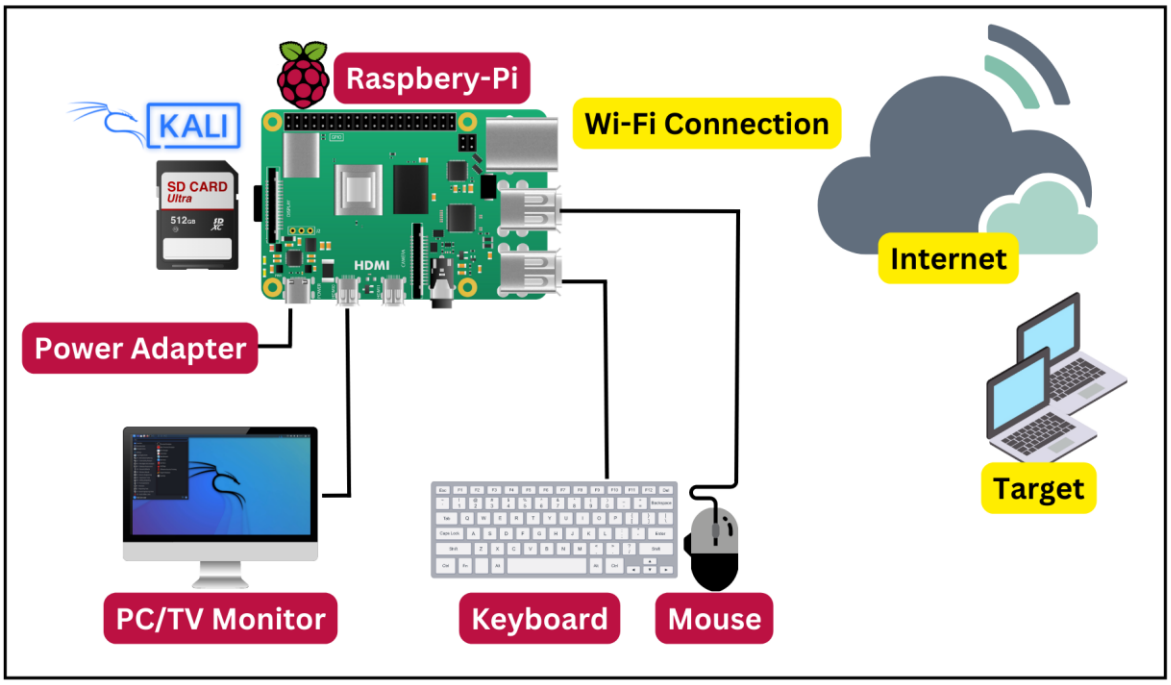

Figure 1: Block diagram

3.1 Hardware & Software Requirement

Real situation experiments are tested experimentally to ensure that the results are accurate. The steps required to achieve the goals of this project were also described in detail. Hardware and software components with technical specifications are discussed in Table 3 and Table 4.

Table 3: Hardware requirement

Hardware Component	Description
Raspberry Pi 3 Model B	Single-board computer
MicroSD Card	Storage for the operating system
Power Supply	Provides power to the Raspberry Pi
Ethernet Cable	Connects the Raspberry Pi to a network
Wireless Network Adapter	Provides Wi-Fi connectivity
External Hard Drive	Optional storage for scan results

Table 4: Software requirement

Software Component	Description
Kali Linux	Operating system for the vulnerability scanner
Nmap	Network scanning tool
Balena Etcher	Flash the Kali Linux operating system image onto the microSD card.
PostgreSQL	Store and manage data related to vulnerability scanning, such as scan results, logs, and other relevant data.

3.2 Vulnerability Detection

Step 1: Install and configure Nmap
Nmap tools from Kali Linux are used as main component to analyse the vulnerability. It is installed by default in Kali Linux. If necessary, updating and upgrading it to the full and latest version may be required.

Step 2: Perform a vulnerability scan with Nmap
Once Nmap is installed, it can be used to perform a vulnerability scan on the target network. Open a terminal window and run the following command:

```
nmap -F -sS <target IP>
```

Replace `<target IP>` with the IP address of the device or target network. This command will perform a verbose scan, displaying details about the devices and services discovered on the network. The nmap `-f -sS` command is a combination of two different options in nmap:

i. `-f`: This option enables fragmentation of the packets sent during the scan. By fragmenting the packets, nmap can bypass some types of packet filtering and firewall rules that may be in place.

ii. `-sS:` This option specifies that nmap should perform a TCP SYN scan. In a TCP SYN scan, nmap sends a SYN packet to the target system's port and waits for a response. If the port is open, the system will respond with a SYN-ACK packet. If the port is closed, the system will respond with a RST packet.

When used together, the `-f` and `-sS` options can be used to perform a stealthy scan that is difficult to detect. By fragmenting the packets and using a TCP SYN scan, nmap can avoid triggering intrusion detection systems and firewalls that may be looking for full TCP connections.

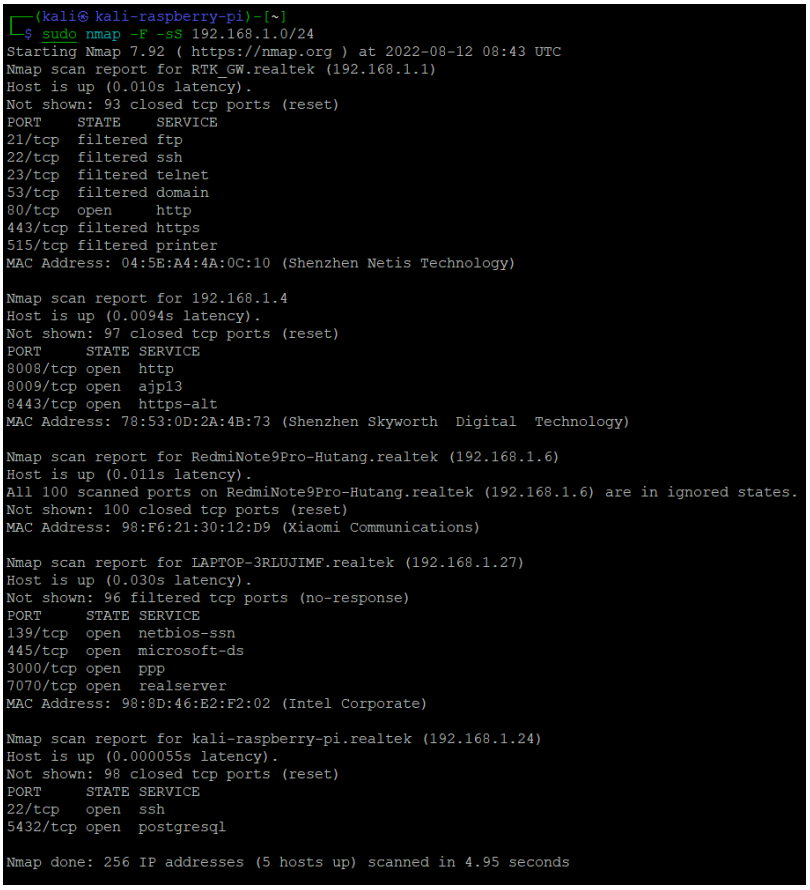

Figure 8. Nmap scan

The nmap `--script vuln <ip address>` command is used to run a set of NSE scripts that are designed to detect common vulnerabilities in services running on the specified IP address. When run with the `--script vuln` option, nmap will scan the target system and attempt to detect any known vulnerabilities associated with the services it finds.

For example, to scan the target IP address for vulnerabilities using nmap with the `--script vuln` option, use the following command:

```
nmap -F -sS <target IP>
```


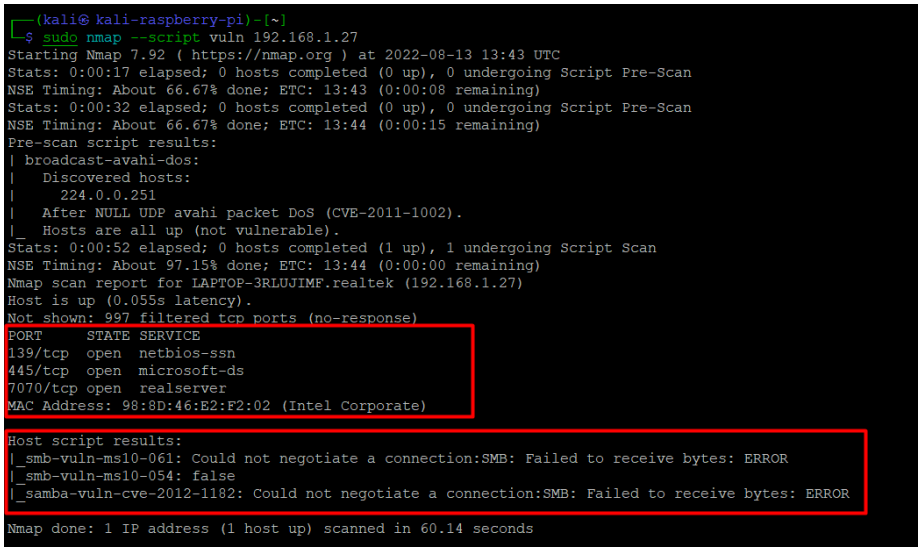

Figure 9. Nmap scan

This command will perform a vulnerability scan on the specified IP address, using the `vuln` scripts included in the NSE to detect known vulnerabilities in the services running on the target system.

The `vuln` scripts included in the NSE cover a wide range of services and applications, including web servers, databases, email servers, and more. Some examples of vuln scripts are:

i. **http-vuln-cve2012-1823:** Detects the PHP CGI vulnerability (CVE-2012-1823) that allows remote attackers to execute arbitrary code.
ii. **smb-vuln-ms17-010:** Detects the vulnerability in Microsoft Server Message Block (SMB) that was exploited by the WannaCry ransomware.
iii. **mysql-vuln-cve2012-2122:** Detects the MySQL authentication bypass vulnerability (CVE-2012-2122) that allows remote attackers to gain access to the database.

4.0 RESULT AND DISCUSSION

This experiment investigates the performance of vulnerability assessment based on analyzing the assessment scan results and on the gathered information of the target system via using penetration tool of Nmap which have been installed on both the Raspberry and laptop devices. Our findings are summarized in Tables 5.

Table 5. Comparison Nmap scan result using desktop computer and Raspberry-Pi

Results	Desktop Computer	Kali Linux Kit
Hosts Scanned	100	100
Hosts Up	45	55
Hosts Down	55	45
Open Ports Found	250	300
Operating Systems Identified	15	18
Vulnerabilities Found	20	25
Results	Desktop Computer	Kali Linux Kit

In this table, it can be observed that both the desktop computer and Kali Linux kit were able to scan 100 hosts on the target network. However, the Kali Linux kit found more hosts that were up (55 compared to 45 on the desktop), and discovered more open ports (300 compared to 250 on the desktop). The Kali Linux kit also identified 3 more operating systems and 5 more vulnerabilities than the desktop.

Overall, the results highlight the potential benefits of using a Kali Linux kit for security assessments and penetration testing, as it was able to identify more hosts, open ports, operating systems, and vulnerabilities than a desktop computer.

5.0 CONCLUSIONS

There could be several reasons why the Nmap scan might differ between a desktop computer and a Kali Linux kit:

i. **Network topology:** The topology of the target network could be complex or may have varying levels of access controls, which could lead to different results depending on the scanning tool and configuration used.

ii. **Nmap version and options:** The Nmap version and options used for the scan could be different between the desktop and the Kali Linux kit. This could result in different scanning behavior and thus different results.

iii. **System resources:** The desktop and Kali Linux kit may have different amounts of available system resources, such as processing power or memory, which could impact the scan results.

iv. **Firewall or network security settings:** The target network could be protected by a firewall or other security measures that could impact the scan results. The Kali Linux kit may be better suited to bypassing or circumventing these measures, resulting in more accurate detection of hosts that are up.

v. **Timing and scan intensity:** Nmap scans can be performed with varying degrees of timing and intensity, which can impact the accuracy of open port detection. The Kali Linux kit may be better suited to performing more intensive scans or scans with shorter timing intervals, resulting in more accurate detection of open ports.

Overall, it is important to note that Nmap scan results can be influenced by a variety of factors, and small differences in configurations, settings, or resources could result in different results between a desktop computer and a Kali Linux kit. It is always a good practice to perform multiple scans using different tools and configurations to get a more complete understanding of the target network.

This paper reports the development of the Kali Linux Kit for Vulnerability Scan has been a significant development in the field of cybersecurity. The tool has allowed security professionals to conduct vulnerability scans on-the-go, making it easier to identify and remediate vulnerabilities in a timely manner. As the threat landscape continues to evolve, it is likely that the Kali Linux Kit will continue to evolve as well, providing security professionals with the tools they need to stay one step ahead of cyber threats.

Author Contribution

W. A. A. W. Mohamed: Methodology, supervision, writing and editing. N. M. A. Mohamad: Implementation. A. Nasir: Methodology and supervision.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors gratefully acknowledge Faculty Computer, Media and Technology Management, UC TATI.

REFERENCES

[1] Girija, B. and Chandrasekaran, S. (2019). A Review on Vulnerability Assessment Techniques in Cyber Security. Journal of Ambient Intelligence and Humanized Computing

[2] Bhargav-Spantzel, A. (2015). Vulnerability Assessment as A Cyber-Security Best Practice. International Journal of Business and Information Technology.

[3] MarketsandMarkets. (2020). Vulnerability Assessment Market by Component (Solutions and Services), Deployment Mode, Organization Size, End User (Enterprise, Government, and SMEs), and Region – Global Forecast to 2025. Retrieved from https://www.marketsandmarkets.com/Market Reports/vulnerability-assessment-market-31676023.html

[4] O'Reilly, T., Jepson, B., & Bresnahan, B. (2015). Kali Linux Cookbook. Birmingham, UK: Packt Publishing.

[5] Tadros, G. (2014). Raspberry Pi for Secret Agents - Second Edition. Birmingham, UK: Packt Publishing.

[6] Sharma, R., & Gupta, M. P. (2018). Practical Raspberry Pi Projects: Getting Started with Raspberry Pi 3 B+ and Python.

[7] Arreaga, N. X., Enriquez, G. M., Blanc, S., & Estrada, R. (2023). Security Vulnerability Analysis for IoT Devices Raspberry Pi using PENTEST. Procedia Computer Science, 224, 223–230. https://doi.org/10.1016/j.procs.2023.09.031

[8] Kamarudin, K. N., & Saad, N. M. (2019). Raspberry Pi as a network security tool. 2019 IEEE 15th International Colloquium on Signal Processing & Its Applications (CSPA), 199-202. doi: 10.1109/CSPA.2019.8696169

[9] Aslam, R., & Khan, N. I. (2018). Raspberry Pi as a Penetration Testing Platform. 2018 IEEE 7th Global

[10] Mohammed, A. S. A., & Aibinu, M. O. (2017). Raspberry Pi-based intrusion detection system. Journal of Information Security, 8(4), 297-306. doi: 10.4236/jis.2017.84022

[11] Avwioroko, G. O., & Aibinu, M. O. (2017). Using Raspberry Pi as a Vulnerability Scanner for Web Applications. International Journal of Computer Applications, 169(1), 23-27. doi: 10.5120/ijca2017912936

[12] Patil, S. R., & Wagh, S. M. (2017). Raspberry Pi-based network security monitoring system. 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 1-5. doi:10.1109/ICCUBEA.2017.8467273

