Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 101-113
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Kali Pi—A Miniature Ultra-Portable Penetration Testing Device

Ahmed Bin Ali

Department of Information Security and Intelligence, Ferris State University, Big Rapids, Michigan, USA
Email: ahmed.b.ali007@gmail.com

How to cite this paper: Ali, A.B. (2025) Kali Pi—A Miniature Ultra-Portable Penetration Testing Device. *Journal of Information Security*, **16**, 101-113.
https://doi.org/10.4236/jis.2025.161005

Received: November 14, 2024
Accepted: December 27, 2024
Published: December 30, 2024

Abstract

Penetration testing plays a critical role in ensuring security in an increasingly interconnected world. Despite advancements in technology leading to smaller, more portable devices, penetration testing remains reliant on traditional laptops and computers, which, while portable, lack true ultra-portability. This paper explores the potential impact of developing a dedicated, ultra-portable, low-cost device for on-the-go penetration testing. Such a device could replicate the core functionalities of advanced penetration testing tools, including those found in Kali Linux, within a compact form factor that fits easily into a pocket. By offering the convenience and portability akin to a smartphone, this innovative device could redefine the way penetration testers operate, enabling them to carry essential tools wherever they go and ensuring they are always prepared to conduct security assessments efficiently. This approach aims to revolutionize penetration testing by merging high functionality with unparalleled portability.

Keywords

Penetration Testing, Portable Device, Cybersecurity, Raspberry Pi

1. Proposal

1.1. Overview

Laptops and computers have long been essential for tasks like penetration testing and ethical hacking. However, technological advancements increasingly emphasize performance improvements and miniaturization. This project focuses on creating an ultra-portable device using the Raspberry Pi, a compact, versatile single-board computer with a 1.2 GHz quad-core processor, 1 GB of RAM, and multiple USB ports. The device will run Kali Linux, the industry-standard penetration testing OS, known for its comprehensive security tools.

The project consists of two phases:

1) Device Construction: A Raspberry Pi will serve as the motherboard, connected to a Wi-Fi card, 3.5- or 5-inch TFT touch display, Bluetooth keyboard and mouse, and powered by a portable battery. A 16 GB SD card will store the Kali Linux OS, functioning as the hard drive.

2) Performance Testing: The device's effectiveness will be evaluated through penetration testing tasks, network monitoring, and Wi-Fi password cracking to assess both its capabilities and potential for misuse.

This project aims to deliver a powerful, portable alternative to traditional penetration testing setups, combining efficiency with convenience.

1.2. Statement of Purpose

This project aims to merge cutting-edge ultra-portable hardware with the world's most advanced penetration testing operating system, creating a powerful synergy between state-of-the-art technology in both hardware and software. Recent advancements in these areas make it possible to deliver premium features at an affordable price, democratizing access to high-quality penetration testing tools.

By developing a dedicated, ultra-portable penetration testing device, this project provides security professionals with a specialized tool tailored for on-the-go testing. Much like digital forensics kits used by investigators, this device can serve as a compact, all-in-one pen-testing kit. Its affordability and portability enable the division of complex penetration testing tasks into manageable sub-tasks, streamlining workflows and reducing the time required for assessments. The potential applications for such devices are vast, offering versatility across the information security landscape, from network defense to educational use, enhancing the efficiency and reach of penetration testers worldwide.

1.3. Research Questions

1) What Footprints can Kali Pi leave in the penetration testing environment?

2) What are the steps to make an ultraportable device that can perform penetration testing like a normal computer or laptop?

3) What is the present state of portable pen testing devices?

4) What purposes can a Kali Pi device be used?

1.4. Contingency Plan

Offensive Security has developed a tailored version of Kali Linux for the Raspberry Pi, optimized to run on devices with at least 512 MB of RAM and a 900 MHz CPU. However, penetration testing often requires significant processing power, especially for resource-intensive tasks like dictionary or brute-force attacks. Limited CPU and RAM on the Raspberry Pi may lead to slower performance or even render some tasks unmanageable. To overcome these limitations, two Raspberry Pi systems can be linked, effectively doubling the available processing power. This configuration enhances the device's ability to handle more demanding tasks, ensuring smoother performance for complex penetration testing activities.

2. Literature Review

2.1. History of Single Board Computers (SBC) and Penetration Testing

Single-board computers (SBCs) are often seen as a modern invention, but the first SBC, the "dyna micro" (later MMD-1), was introduced in 1976 by E&L Instruments. Based on Intel architecture, it integrated I/O, display, memory, and user input onto a single board. SBCs faced challenges in the late 20th century due to limited miniaturization and high costs, with personal computers focusing more on motherboards connected to daughterboards for I/O functions.

The 1960s marked the beginning of computer security as network access expanded, introducing new threats. In 1967, the term "penetration" was coined to describe system attacks, highlighting the need for penetration testing to identify vulnerabilities and improve security [1]. James P. Anderson, a leading expert in the field, outlined six key stages of an attack:

- Identifying vulnerabilities
- Designing an attack
- Testing the attack
- Seizing a communication line
- Executing the attack
- Exploiting the entry

These early developments laid the foundation for modern penetration testing practices.

2.2. Growth of Single Board Computers and Penetration Testing

The demand for single-board computers (SBCs) grew from efforts by companies like Raspberry Pi, BeagleBoard.org, and Arduino in the 2000s, which developed affordable, user-friendly microcontrollers. This led to wider adoption and reduced prices for SBCs and Systems on Chip (SoCs) [2]. The 2011 release of the $35 Raspberry Pi, designed by a University of Cambridge team for students to learn programming, revolutionized computing and gained global popularity [3]. Penetration testing evolved from early tools like Multics in the 1960s to the 1990s SATAN, which paved the way for Nmap and Nessus. In 2006, Offensive Security launched BackTrack, which evolved into Kali Linux in 2013. Now, Kali Linux is the leading OS for penetration testing, offering tools like Nmap, Wireshark, and Metasploit [4].

Combining Raspberry Pi with Kali Linux provides a portable, high-performance solution for penetration testers, bridging the gap between portability and capability while making advanced tools more accessible.

2.3. Raspberry Pi v/s Personal Computers

"Many of today's SBCs have become so powerful that they are beginning to rival modern PCs and tablets."—Cliff Ortmeyer, Global Head of Solutions Development.

This statement reflects the growing computational power of single-board computers (SBCs) in modern technology. The introduction of the Raspberry Pi marked a significant shift, miniaturizing computing to the size of a credit card without sacrificing functionality. With the release of the Raspberry Pi 3 in 2016, SBCs began offering performance on par with personal computers, featuring a quad-core ARM Cortex-A53 CPU, 1 GB of RAM, and improved I/O capabilities. By using an SD card as a bootable storage device and installing Kali Linux, the Raspberry Pi can be transformed into a compact, portable platform for penetration testing or digital forensics,

2.4. Raspberry Pi v/s Other SBCs

The Raspberry Pi is a credit-card-sized microcomputer, or single-board computer (SBC), developed by educators to provide an affordable platform for students to learn programming. Initially proposed in 2006 and based on the Atmel ATmega644 microcontroller, it was released to the public after five years of development [5].

The Raspberry Pi's launch triggered strong demand for miniature SBCs and spurred competition. BeagleBone was the first major competitor to release its own SBC, followed by other products like RloTBOARD and PANDABOARD ES. However, the Raspberry Pi quickly became the market leader, selling over two million units in its first two years. While BeagleBone's SBC launched the same year, it failed to match the Raspberry Pi's popularity. Despite offering similar specs, RloTBOARD and PANDABOARD ES struggled to gain traction, leaving Raspberry Pi and BeagleBoard as the dominant players in the SBC market.

2.5. Kali Linux v/s Backbox

Kali Linux's main competitor, Backbox, was released in 2010 as an alternative to Kali (formerly BackTrack). Both are well-regarded in the cybersecurity community, but they differ in capabilities and features.

Capability Set: Kali Linux stands out with an extensive collection of over 600 preloaded tools, compared to just over 70 tools in Backbox. This vast toolkit gives Kali Linux a significant edge, as it covers a wide range of tasks such as penetration testing, digital forensics, network analysis, and vulnerability assessment. This comprehensive set allows security professionals to tackle a diverse array of challenges in one unified environment [6].

Graphical User Interface (GUI): Kali Linux's GUI is designed to be intuitive and user-friendly, making it easier for both novice and experienced users to navigate. The interface is streamlined for efficient task management, with customizable options for accessibility and workflow optimization. In contrast, Backbox's GUI is more traditional and can be more challenging for new users, particularly those who require faster access to penetration testing tools [6].

Vulnerabilities: When it comes to security, Kali Linux is generally considered more secure, with only 85 documented vulnerabilities in the CVE database. Backbox, on the other hand, has 422 vulnerabilities, which could pose a higher risk to users relying on it for critical security tasks. Kali Linux's lower vulnerability count reflects its continuous updates and dedicated focus on secure development practices.

Incident Response: Kali Linux excels in incident response, as it is equipped with a wide array of tools that facilitate quick detection, analysis, and mitigation of security incidents. With tools like The Sleuth Kit, Volatility, and Autopsy, Kali Linux provides a comprehensive set of forensic and incident response capabilities. In comparison, Backbox offers fewer specialized tools for incident response, making it less versatile in handling real-time security events or post-incident investigations.

In summary, Kali Linux's greater toolset, enhanced user interface, robust security, and specialized incident response capabilities make it the preferred choice for penetration testers, digital forensics experts, and cybersecurity professionals. Its ongoing development ensures that it stays at the forefront of security, providing users with the most advanced tools available in the field.

2.6. Future of Kali Pi Device

We live in a digital age where everything—from bank transactions to personal photos—is stored online, thanks to years of global research and development. However, this progress brings growing concerns over digital security. A recent RAND report shows that 65 million Americans fall victim to data breaches annually, contributing to billions in cybercrime losses. With over $6.4 billion spent each year on security checks and penetration testing, the Kali Raspberry Pi offers a cost-effective solution. By using multiple devices, organizations can reduce downtime and improve efficiency, saving both time and money while handling resource-intensive tasks [2].

Kali Pi devices are versatile tools that can be employed for a wide range of purposes in the field of cybersecurity and penetration testing. Below are some key uses:

1) Proactive Security: Kali Pi is perfect for penetration testing, enabling security teams to identify and fix vulnerabilities with tools like Wireshark, Nmap, Nessus, Metasploit, and John the Ripper for comprehensive scans and simulated attacks.

2) Reactive Security: In incident response, Kali Pi helps trace attack footprints and analyze breaches using Kali Linux's forensic tools, such as RAM forensics, password recovery, and network forensics, to identify threats and recover data.

3) Wireless Security: Kali Pi excels in Wi-Fi security testing, using tools like Aircrack-ng to audit network vulnerabilities, crack passwords, and test encryption protocols for weaknesses.

4) Network Monitoring: With tools like Wireshark and tcpdump, Kali Pi enables real-time network traffic analysis to detect unauthorized activity and ensure

network health.

5) Malware Analysis: The Kali Pi can dissect suspicious files and study malware behavior with tools like Cuckoo Sandbox and Volatility, aiding in threat detection and mitigation.

6) Social Engineering Testing: Using tools like SET (Social Engineering Toolkit), Kali Pi can simulate phishing and spear-phishing attacks to test defenses and improve employee awareness.

Overall, the Kali Pi device is a powerful, portable tool for penetration testing, incident response, wireless security, malware analysis, and network monitoring, providing a cost-effective solution for cybersecurity professionals.

2.7. Potential Misuses of Kali Pi Device

The Kali Pi device, while a powerful tool for legitimate penetration testing and security assessments, also has the potential to be misused if it falls into the wrong hands. Here are some ways in which the device could be exploited for malicious purposes:

Unauthorized Testing: It could be used to hack systems or networks without permission, leading to data theft or service disruptions.

Wi-Fi Hacking: Tools like Aircrack-ng and Wireshark could enable Wi-Fi network breaches and data interception.

Password Cracking: Tools such as John the Ripper can be used to crack passwords and gain unauthorized access.

Exploiting Vulnerabilities: Kali Pi could exploit system vulnerabilities using tools like Metasploit to gain control over devices.

Social Engineering: The device could be used to create phishing sites or social engineering attacks to steal credentials.

Botnet Creation: It could be part of a botnet for launching DDoS attacks or other malicious actions.

Surveillance: Kali Pi can be used for packet sniffing and tracking online activity, violating privacy.

Malware Deployment: It could deploy malware onto vulnerable systems via USB or network attacks.

By following these guidelines, you can create a highly functional and portable Kali Pi device for effective penetration testing.

3. Methodology

3.1. Overview

This chapter will detail the approach to implementing the project to address the research questions related to this study. The research is conducted under the interpretative paradigm, as the research questions are open-ended. Through extensive online research, I gained an in-depth understanding of single-board computers and how to convert them into portable penetration testing devices. This research helped me develop the approach I will take to tackle the research questions and challenges associated with the miniature ultra-portable penetration testing device. In this chapter, I will analyze the role of the Raspberry Pi in a penetration-testing environment and outline the steps involved in creating an ultra-portable penetration-testing device. Additionally, I will discuss the purposes and applications of these devices in the modern computing world.

3.2. Research Strategy

This research will utilize an observational study methodology to address the research questions. Observations will be conducted during the implementation of the project, and careful notes will be taken to ensure accurate answers to the research questions outlined in the proposal.

3.3. Research Approach & Findings

1) What Footprints can Kali Pi leave in the penetration testing environment?

Footprinting is a method of gathering information about a computer system and its entities. Every device in the modern computing world has footprints and these footprints can be gathered by using different computer security tools like Nmap, ping sweeps, OS fingerprinting, TCP/UDP scans, network enumeration, and Net Discover.

To discover the footprints of the Raspberry Pi system, the following seven steps should be performed:

a) Information gathering

b) Determining the network range

c) Identifying active machines

d) Finding open ports and access points

e) OS fingerprinting

f) Fingerprinting services

g) Mapping the network

Kali Pi functions like any full-fledged pen-testing system, leaving footprints in the testing environment that must be managed carefully. A well-planned strategy is crucial to minimize or eliminate these traces. Although initial Nmap scans failed to detect the Kali Pi's OS, Wireshark successfully identified network activity. Kali Pi is designed as a portable, cost-effective alternative to larger, pricier devices that are harder to transport and use.

2) What are the steps to make an ultraportable device that can perform penetration testing like a normal computer or laptop?

Creating an ultra-portable penetration testing system like Kali Pi requires balancing size and power. Key factors include:

Computing Power: A powerful processor and sufficient RAM to handle pen-testing tasks.

Power Supply: An internal battery with a long life to ensure portability without a constant power source.

Input Mechanism: A touchscreen or Bluetooth-enabled keyboard for easy input and output.

However, creating Kali Pi involves challenges. Kali Linux supports Raspberry Pi but lacks display drivers, requiring an HDMI connection that conflicts with portability. Additionally, the OS doesn't come with pre-installed tools, requiring manual installation of meta-packages. To be fully functional, Kali Pi needs a version of Kali Linux with display drivers and pre-installed tools.

3) What is the present state of portable pen-testing devices in 2016?

In 2016, laptops were the primary portable devices for penetration testing due to their power and battery life, but they are expensive and not highly portable. This project aims to create a device that is 10 times smaller yet retains all the capabilities of a laptop, revolutionizing penetration testing. If successful, this ultra-portable device could set a new standard. While penetration testing tools have evolved, hardware has largely stayed the same. Kali Pi addresses this by reducing the device size by 80% and weighing just 0.4 pounds, making it a major leap forward in portability for pen-testers.

4) What purposes can a Kali Raspberry Pi device be used?

Kali Linux operating system installed on a Raspberry Pi system, in theory, can be used as a replacement for the current devices that are used for performing penetration testing like laptops and personal computers but the practicality of this theory is yet to be tested. Kali Linux Raspberry Pi will be tested based on the following phases:

a) Foot Printing

b) Scanning

c) Enumeration

d) Vulnerability scanning

e) Exploiting vulnerabilities

f) Maintaining access

Kali Pi aims to replace traditional penetration testing tools by handling essential tasks like footprinting, scanning, and enumeration. It will also perform vulnerability scans, exploit weaknesses, and maintain access. Affordable and ultra-portable, Kali Pi is accessible to all skill levels and enables simultaneous testing across multiple devices for improved efficiency, making it a potential game-changer in penetration testing.

4. Project Implementation

4.1. Phase 1: Developing Kali Pi

Kali Pi is built on the Raspberry Pi 3, which has the Kali Linux 2.0 operating system installed. Kali Pi consists of various hardware and software components and nearly all of these components need to be configured, making it a rather tedious task.

The following are the hardware requirements to build a micro-computer:

Raspberry Pi 3 (Model B) (see **Figure 1**).

To develop a Kali Pi, it is essential to have a powerful processor and sufficient RAM, as penetration testing tasks can be quite resource-intensive. The most powerful version of the Raspberry Pi single-board computer is the Raspberry Pi 3 Model B, which is based on ARM architecture.

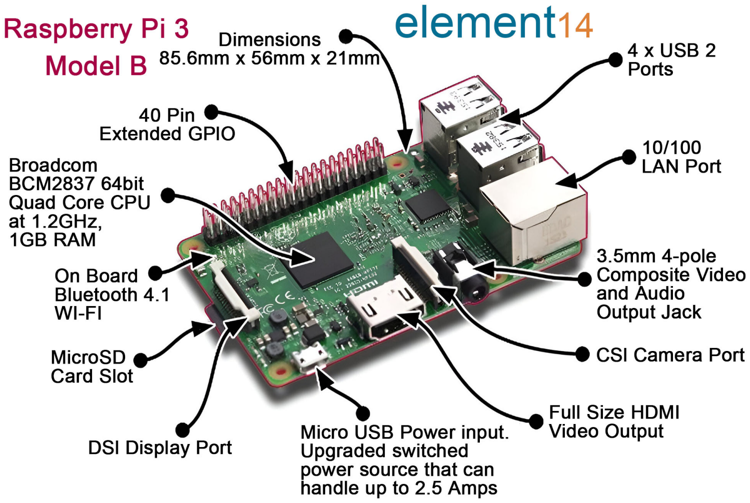


Figure 1. Raspberry Pi 3.

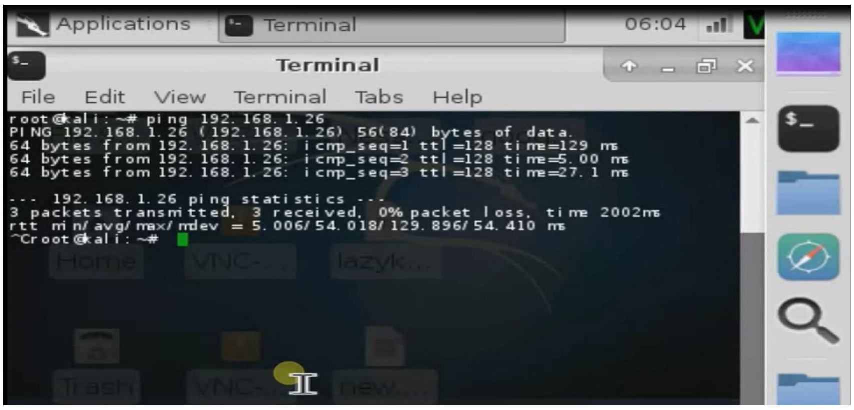
4.2. Phase 2: Installing Kali Linux and Tools

Kali Linux can be downloaded from the official website, with a version tailored for Raspberry Pi models based on ARM architecture. This version is designed for headless setups, and additional drivers are required to use it with a display.

Installing Kali Linux on a Raspberry Pi can be challenging, but Osoyoo.com simplifies the process by offering a version with pre-installed KeDei display drivers. To install, use tools like Win32DiskImager to write the image to a Micro SD card, which serves as the Raspberry Pi's storage. The base Kali Linux image doesn't include penetration testing tools. To access the full suite, you'll need to download and install a meta-package from the Kali Linux website.

4.3. Phase 3: Performing Penetration Testing

Target Discovery: To discover the target machine a PING is sent for the Kali Pi device as shown in Figure 2.



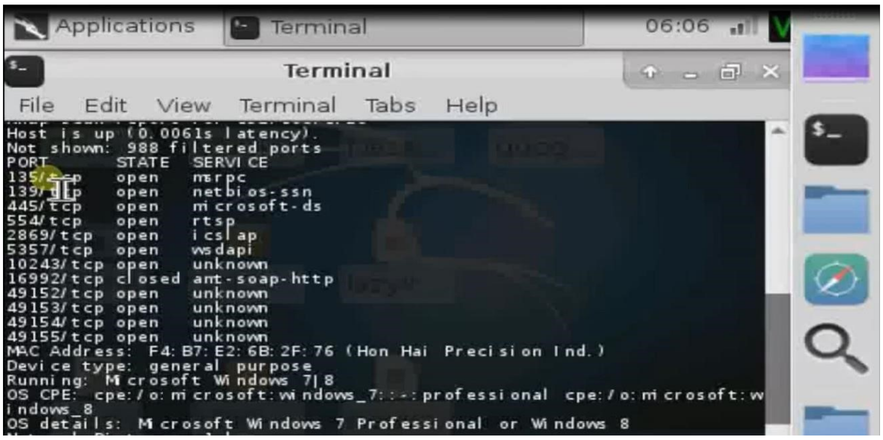
```
root@kali:~# ping 192.168.1.26
PING 192.168.1.26 (192.168.1.26) 56(84) bytes of data.
64 bytes from 192.168.1.26: icmp_seq=1 ttl=128 time=129 ms
64 bytes from 192.168.1.26: icmp_seq=2 ttl=128 time=5.00 ms
64 bytes from 192.168.1.26: icmp_seq=3 ttl=128 time=27.1 ms

--- 192.168.1.26 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.006/54.018/129.896/54.410 ms
^Croot@kali:~#
```

Figure 2. Ping.

Host Enumeration: To gather information about the target machine, conduct an Nmap scan focused on identifying the operating system as shown in Figure 3. This scan can reveal important details about the target's operating system, which can be beneficial during the exploitation phase of penetration testing.

Command Line: Nmap-O 192.168.1.26

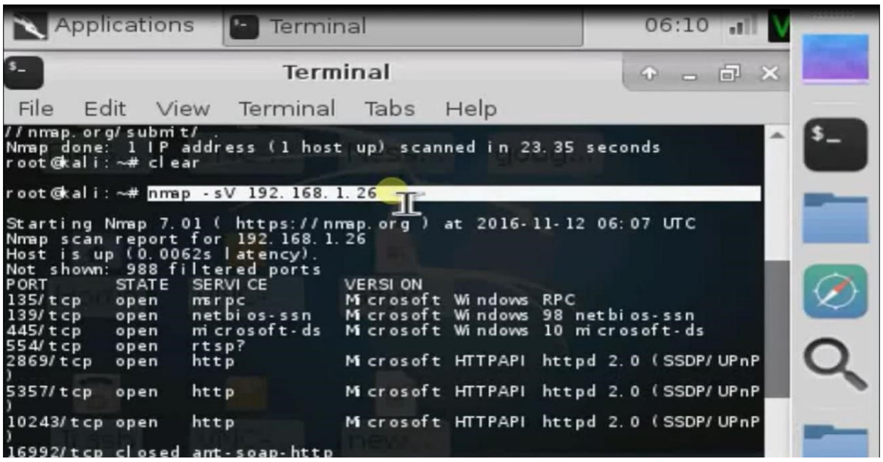


```
Host is up (0.0061s latency).
Not shown: 988 filtered ports
PORT      STATE  SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
554/tcp   open   rtsp
2869/tcp  open   icslap
5357/tcp  open   wsdapi
10243/tcp open   unknown
16992/tcp closed amt-soap-http
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp open   unknown
MAC Address: F4:B7:E2:6B:2F:76 (Hon Hai Precision Ind.)
Device type: general purpose
Running: Microsoft Windows 7|8
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:w
indows_8
OS details: Microsoft Windows 7 Professional or Windows 8
```

Figure 3. OS scan.

Port Scanning: Nmap can be utilized to scan ports and identify the services running on them, as well as their versions as shown in Figure 4. A service version scan was conducted, resulting in a list of open ports along with the corresponding services and their respective versions.

Command Line: Nmap-sV 192.168.1.26



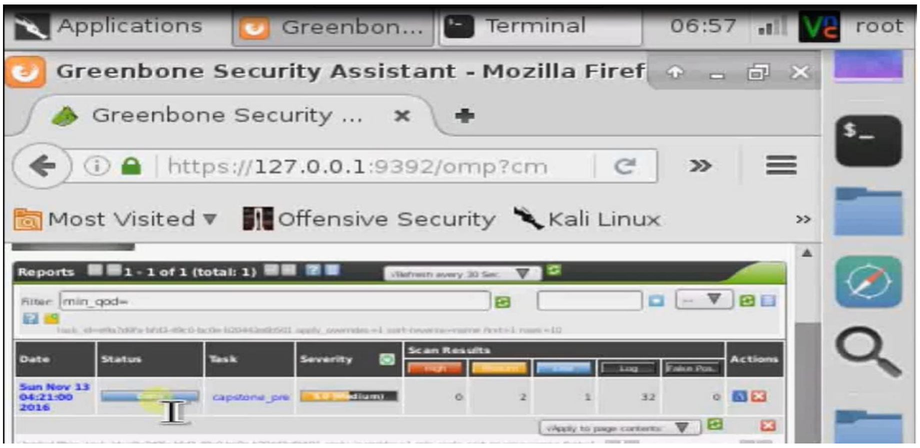
```
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.35 seconds
root@kali:~# clear

root@kali:~# nmap -sV 192.168.1.26

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-12 06:07 UTC
Nmap scan report for 192.168.1.26
Host is up (0.0062s latency).
Not shown: 988 filtered ports
PORT      STATE  SERVICE       VERSION
135/tcp   open   msrpc         Microsoft Windows RPC
139/tcp   open   netbios-ssn   Microsoft Windows 98 netbios-ssn
445/tcp   open   microsoft-ds  Microsoft Windows 10 microsoft-ds
554/tcp   open   rtsp?
2869/tcp  open   http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP
)
5357/tcp  open   http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP
)
10243/tcp open   http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP
)
16992/tcp closed amt-soap-http
```

Figure 4. Service version scan.

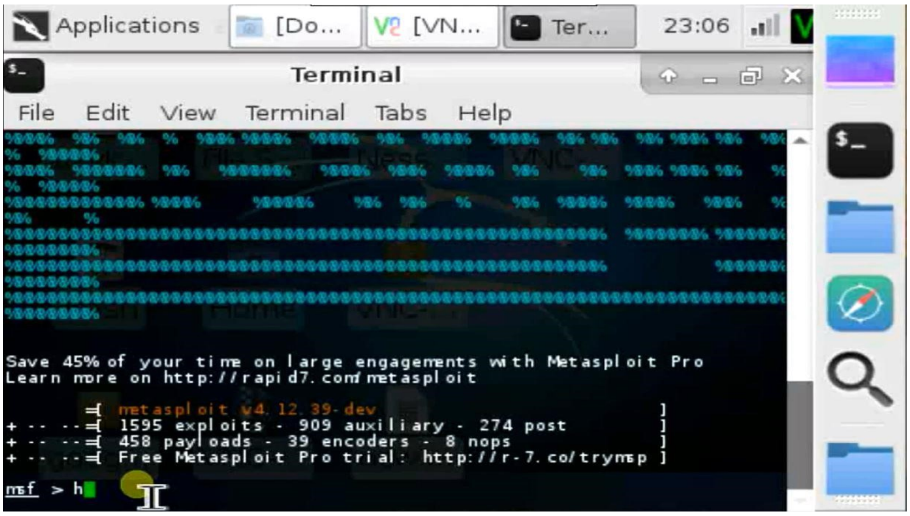
Vulnerability scanning: After completing the host enumeration phase, the next logical step was to perform a vulnerability scan as shown in Figure 5. The OpenVAS vulnerability scanner package was downloaded and installed on the Kali Pi device. OpenVAS was then used to conduct a vulnerability scan, which generated a list of vulnerabilities and logs that could potentially be exploited on the system.



Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Sun Nov 13 04:21:00 2016	[illegible]	capstone_pre	5.0 (Medium)	0	2	1	32	0	

Figure 5. OpenVas vulnerability scan.

Exploitation: Kali Pi is a device that works as a normal system and can be used for all the tasks of penetration testing as shown in Figure 6. Tools like Metasploit can be used to exploit the vulnerabilities of the target system.



```
Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.39-dev                          ]
+ -- --=[ 1595 exploits - 909 auxiliary - 274 post         ]
+ -- --=[ 458 payloads - 39 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > h
```

Figure 6. MSF console.

5. Recommendations and Conclusions

5.1. Recommendations

Creating a Kali Pi device can be a challenging and time-consuming process, even with thorough research. The key to success lies in selecting the right hardware and penetration testing tools. Here are some essential recommendations for building a portable penetration testing device:

- Use the Latest Technology: Always opt for the latest hardware, as newer technology often outperforms older generations. For example, the Raspberry Pi 3 was one of the best SBCs available in 2016.
- Ensure Compatibility: Choose hardware that is supported by the software you plan to install. Kali Linux, for instance, offers an OS version specifically compatible

with Raspberry Pi 3.

- Prioritize Compact, High-Power Components: Select smaller, high-performance components for the battery, display, and enclosure to keep the device compact and portable.
- Add Heat Sinks: Penetration testing can be resource-intensive and may cause overheating. Installing heat sinks on the SBC will help prevent potential malfunctions.
- Research the OS and Display Compatibility: Many operating systems are designed to run headless (without a display). Ensure the OS you choose includes the necessary drivers for your display.
- Be Cautious When Installing Tools: The process of downloading and installing penetration testing tools can be lengthy. Carefully select the tools you need to avoid overwhelming your device's storage or memory. Downloading a meta-package suited to your needs can save space and improve efficiency.
- Invest in a Wireless Keyboard and Mouse: Since smaller displays can limit navigation, a wireless keyboard and mouse will make command input and system control easier.
- Leverage Online Resources: If you encounter challenges during development, Google can be an invaluable tool for troubleshooting and finding solutions.
- By following these guidelines, you can create a highly functional and portable Kali Pi device for effective penetration testing.

5.2. Conclusion

The information security industry primarily focuses on software and tools, with significant emphasis placed on developing resources for penetration testers. However, the hardware used in this field receives comparatively little attention. Consequently, the development of hardware is largely reliant on companies that manufacture personal computers, which are not specifically designed as penetration testing devices. Kali Pi addresses this issue by providing software and hardware improvements tailored specifically for penetration testing. It is the most affordable device capable of performing pen-tests and is designed for students and novice pen-testers who are starting to explore the expansive world of information security. In today's rapidly evolving technological landscape of information security and intelligence, Kali Pi represents an important advancement in the right direction.

Funding

This research did not receive any specific grants from funding agencies in public, commercial, or not-for-profit sectors.

Author Contributions

The author independently developed the research idea, carried out the study, and composed the entire manuscript.

Conflicts of Interest

The author states there are no conflicts or competing interests related to this work.

References

[1] Raspberry Pi Foundation (2012) About Us. https://www.raspberrypi.org/about/

[2] Upguard (n.a.) Kali Linux vs. Backbox: Pen Testing and Ethical Hacking Linux Distros. https://www.upguard.com/blog/kali-linux-vs-backbox-pen-testing-ethicalhacking-linux-distros

[3] Hymel, S. (2015) Benchmarking Single Board Computers. https://www.sparkfun.com/news/1888

[4] Lee, M. (2015) Meet the Future: Single-Board Computers. http://it.toolbox.com/blogs/this-is-it/meet-the-future-singleboard-computers-68451

[5] INFOSEC (2016) The History of Penetration Testing. http://resources.infosecinstitute.com/the-history-of-penetration-testing/

[6] Linux (2012) About Kali Linux. https://www.kali.org/about-us/