



# **A Review and Comparison of Penetration Testing Operating Systems for the Raspberry Pi**

**Ellora James**

CMP320: Ethical Hacking 3

BSc Ethical Hacking Year 3

2020/21

*Note that Information contained in this document is for educational purposes.*

# Abstract

---

Raspberry Pi's are popular micro-computers in the digital making community, but their low cost, versatility and discreteness also make them excellent tools for beginner and professional ethical hackers. Cybercrime is on the rise and combined with the preexisting shortage of cybersecurity professionals, more people must be encouraged into the profession. But for beginners who have limited or no access to specialist tools, equipment or training, the legal aspects of ethical hacking can make it a difficult skill to simply try at home.

This is where Raspberry Pi's come in, their affordability makes them an accessible investment for beginners, and there are various tools and operating systems out there that can be used to practice penetration testing.

In this paper, three penetration testing operating systems designed specifically for the Raspberry Pi were reviewed to establish which is the best ethical hacking on the Raspberry Pi, with a focus on beginner friendliness. Each operating system was installed, run on a Raspberry Pi and a basic web application attack was carried out to test some of the tools available and how well they performed.

Comparisons were made based on factors including documentation, tools available and how long scans took. A conclusion was then made combining all the factors to determine which of the three operating systems was best suited for ethical hacking on the Raspberry Pi.

# +Contents

---

1	Introduction .....	1
1.1	Background .....	1
1.2	Operating Systems/Suites.....	2
1.2.1	Kali Linux .....	2
1.2.2	Sticky Fingers Kali-Pi.....	2
1.2.3	PwnPi.....	2
1.3	Aim .....	3
2	Procedure.....	4
2.1	Overview of Procedure .....	4
2.2	RasPwn OS .....	5
2.3	Kali Linux .....	5
2.3.1	Installation .....	5
2.3.2	Tools Test .....	6
2.4	Sticky Fingers Kali-Pi.....	9
2.4.1	Installation .....	9
2.4.2	Tools Test .....	12
2.5	PwnPi.....	15
2.5.1	Installation .....	15
2.5.2	Tools Test .....	17
3	Results.....	21
3.1	Review Factor Scores .....	21
3.1.1	Kali Linux .....	21
3.1.2	Sticky Fingers Kali-Pi.....	21
3.1.3	PwnPi.....	22
3.1.4	Overall.....	22
3.2	Scan Times Comparison .....	23
3.2.1	Nmap Scan .....	23
3.2.2	Nikto Scan .....	23
3.2.3	sqlmap Scan .....	24
3.2.4	John the Ripper .....	24
4	Discussion.....	25

4.1	General Discussion.....	25
4.1.1	Review Factor Scores .....	25
4.1.2	Scan Times.....	26
4.2	Conclusions .....	26
4.3	Future Work.....	27
	References .....	28
	Appendices.....	30
	Appendix A – Kali Linux Nmap Scan .....	30
	Appendix B – Kali Linux Nikto Scan .....	32
	Appendix C – Sticky Fingers Kali-Pi Nmap Scan .....	33
	Appendix D – Review Factor Grading Rubrics.....	35

# 1 INTRODUCTION

## 1.1 BACKGROUND

---

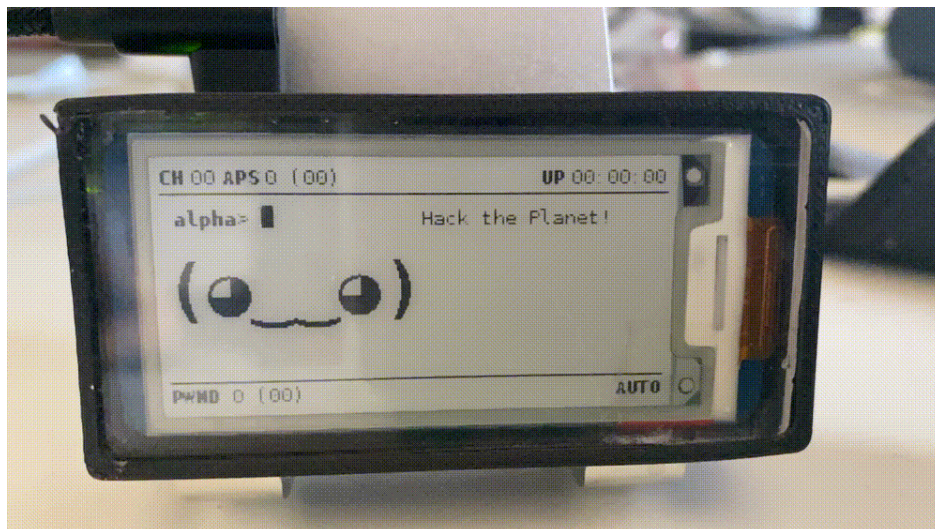
The Raspberry Pi is a cost-effective micro-computer designed for digital making. Its low price, portability, and ability to interact with a variety of platforms makes it a staple in the digital making community. It is also commonly used in the education system as a low-cost way to encourage children to explore programming and general computer science. (Raspberry Pi Foundation, n.d.)

The Raspberry Pi Foundation, the charity behind the computer, aim 'To put the power of computing and digital making into the hands of people all over the world' (Raspberry Pi Foundation, n.d.). They focus on making computing accessible to all and fostering a collaborative community space.

To date, the foundation has sold over 37.4 million Raspberry Pi computers (Raspberry Pi Foundation, 2020) and, as of early 2020, are the seventh most used platform among software developers across the world (Stack Overflow, 2020).

It is no surprise then that their popularity has also made its way into the ethical hacking space. Their portability and discreetness make them useful for professionals, but it is their low-cost and active community that make them excellent tools for those looking to hone security skills.

One well-known example of this is the Pwnagotchi. A portmanteau of 'Pwn' and 'Tamagotchi', this digital pet 'eats' Wi-Fi handshakes and uses machine learning to maximize the amount of material it captures.



*Figure 1. The Pwnagotchi (Margaritelli, n.d)*

Once captured, users can view the material and use other tools to crack the handshakes.

The Pwnagotchi uses the Raspberry Pi Zero (WiFi) for the aforementioned reasons. It is used by both professional hackers and digital making hobbyists alike, but its creator Simone Margaritelli designed it specifically as a tool for anyone interested in learning to hack. (Franceschi-Bicchierai, 2019)

According to the International Information System Security Certification Consortium, in 2020 there was a global cybersecurity workforce gap of 3.12 million ((ISC)<sup>2</sup>, 2020). There was also an increase in the number of organizations worldwide who reported a data breach, from 84% in October 2019 to 94% in June 2020 (VMware, Inc., 2020). These statistics show a clear need for more cyber-security professionals.

This is where the Raspberry Pi has the potential to be a powerful tool in helping to close the gap. Learning ethical hacking usually requires specialist tools and many techniques need to be practised in a secure environment to avoid legal issues or damage. The affordability and accessibility of the Raspberry Pi make it ideal for beginners and there are several operating systems specifically designed for learning ethical hacking on the Pi.

## **1.2 OPERATING SYSTEMS**

---

Three operating systems were selected for review in this paper. Whilst there are other security-based operating systems available, these were chosen as they have been designed specifically for the Raspberry Pi.

### **1.2.1 Kali Linux**

Kali Linux is a popular Debian-based security distribution that is designed to be used for penetration testing, security research, computer forensics and reverse engineering. It comes with a huge variety of tools and is a staple in the security community. The version reviewed in this whitepaper is one specifically built for the Raspberry Pi. (Kali Linux, n.d.)

### **1.2.2 Sticky Fingers Kali-Pi**

Sticky Fingers Kali-Pi, or just Kali-Pi, is a version of Kali-Linux that is optimized for use with touch screens. The basic installation comes with a slimmed-down version of the Kali-suite and has full Raspberry Pi 4 support. (Re4son, 2018)

### **1.2.3 PwnPi**

PwnPi is a penetrating testing operating system built on a basic version of Debian Wheezy for the Raspberry Pi. It comes with more than 200 security tools and uses OpenBox for window management. (PwnPi, n.d.)

## 1.3 AIM

---

This project aims to review several operating systems that have been designed for use with the Raspberry Pi. They will be reviewed on the following aspects, with a focus on beginner friendliness:

- Ease of installation
- Documentation available
- Ease of use
- Tools Available
- Performance
- Any other notable features

Comparisons will then be drawn from these factors to establish which operating system is the most suitable for beginners to ethical hacking.

## 2 PROCEDURE

### 2.1 OVERVIEW OF PROCEDURE

---

The following procedure documents the installation process of all the operating systems, along with a basic penetration testing exercise to test a handful of the tools present.

For a fair comparison, all operating systems were installed onto the same brand and size of SD card. These were the Gigastone 32GB micro SD cards.

All operating systems were used and tested on a Raspberry Pi 3 Model B v1.2 using the official Raspberry Pi power supply.

A vulnerable image used to test the tools, RasPwn OS, was installed on an 8GB SD card and run using a Raspberry Pi 2 Model B v1.1. RasPwn OS is a Linux distribution that uses a Raspberry Pi to emulate a vulnerable Linux server. (RasPwn OS, 2016)

To test some of the tools, a small attack was carried out on the Damn Vulnerable Web Application hosted on RasPwn OS. Two separate scans were run against the network using Nmap and Nikto.

Nmap (Network Mapper), is a tool used for network security auditing. It can be used to determine hosts on the network, operating systems in use, version numbers, firewalls and much more. (Nmap, n.d.)

Nikto is another web server scanner that can search for dangerous files/programs, version-specific issues and outdated versions on a server. (Kali Tools, 2014)

Wireshark and sqlmap were then used to brute force SQL injection on one of the pages. Wireshark is a popular network protocol analyzer that can inspect protocols, perform live capture and much more (Wireshark Foundation, n.d.). sqlmap is a penetration testing tool that can be used to automatically exploit many different SQL injection flaws. (Guimaraes & Stampar, 2021)

Finally, John the Ripper was used to crack the password hashes acquired from the SQL brute force. John the Ripper is a password security auditing and recovery tool that can be used to crack many different hash types. (openwall, n.d.)

To install all the operating systems, the Raspberry Pi Imager program was used. This was downloaded from the Raspberry Pi site. (Raspberry Pi, n.d.)



## 2.2 RASPWN OS

To test some of the tools included within the following operating systems, a vulnerable web server was set up to act as a target for these scans.

The operating system was downloaded as a ZIP archive from the RasPwn OS website and then written to an SD card using the Raspberry Pi imager.

The Pi was then loaded with the SD card and booted headless.

Once booted the OS could be connected to via the WiFi 'RasPwnOS' with the password 'In53cur3!'.

## 2.3 KALI LINUX

### 2.3.1 Installation

Kali Linux has distributions designed specifically for the Raspberry Pi. Whilst the Raspberry Pi 3 being used could run a 64-bit OS, the website recommended the 32-bit version as it had more documentation and was more widely recognised. (Kali Linux, n.d.)

#### RASPBERRYPI FOUNDATION

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux RPI (img.xz)	Torrent	2021.1	1.9G	d471c2a03462b0eef098da38190808b1a3207b27cb7c20e0caaa1bac80d18812
Kali Linux RaspberryPi 2, 3, 4 and 400 (img.xz)	Torrent	2021.1	2.1G	ead2ebf6638a8f454b9259a5a395d48420888c955f8f3b0147808da7cc0a2b07
Kali Linux RaspberryPi 2 (v1.2), 3, 4 and 400 (64-Bit) (img.xz)	Torrent	2021.1	2.1G	f5e126f33d32882f526e16b5148bd8b84a4e7c351bdd0eb9cfe3da2176580181
Kali Linux RaspberryPi Zero/Zero W (img.xz)	Torrent	2021.1	2.0G	fff1175a7d3809e7a3fac35f987ac534ffc1c36c2d13d79b405aaf5464c6d54f

Figure 2. Kali Linux download for the Raspberry Pi.

The image was downloaded from the offensive-security page and then written to the SD card using the Raspberry Pi imager.

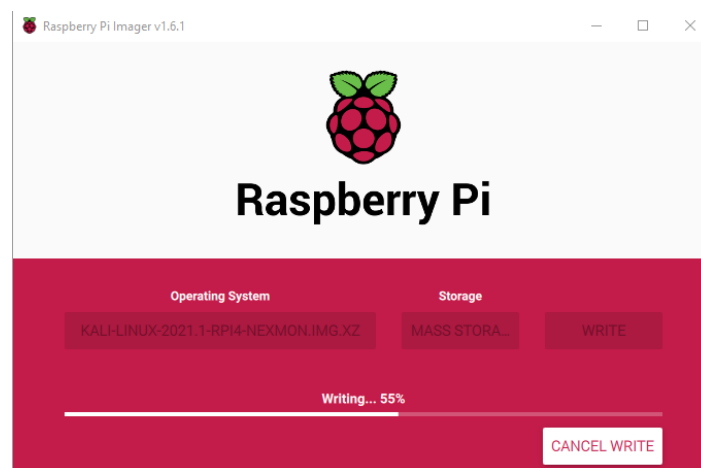


Figure 3. Using the Raspberry Pi imager to write the operating system to the SD card.

The SD card was then loaded into the Pi and the operating system booted successfully. When logging in for the first time the default Kali username and password of 'Kali' did not work. It took some educated guesses to figure out that the login details were 'Kali' and 'password'. These did not appear to be written on the website anywhere.

## 2.3.2 Tools Test

### 2.3.2.1 Nmap

An Nmap scan was run against 'playground.raspwn.org' using the following command: 'Nmap -v -A playground.raspwn.org'

```
kali@kali:~$ nmap -v -A playground.raspwn.org
```

Figure 4. Nmap command.

The full output of the scan can be found in Appendix A.

As expected, the scan identified several flaws with the applications present on the RasPwn server. The scan was completed in 89.45 seconds with no issues.

### 2.3.2.2 Nikto

A Nikto scan was also run against RasPwn using the following command: 'nikto -h playground.raspwn.org'

```
kali@kali:~$ nikto -h playground.raspwn.org
```

Figure 5. Nikto command.

The full output of the scan can be found in Appendix B.

The scan found numerous issues with the web applications and took 2364 seconds to complete.

### 2.3.2.3 Wireshark & sqlmap

To demonstrate a direct attack, sqlmap was used against the Damn Vulnerable Web Application (DVWA).

The DVWA was located at 192.168.99.13/dvwa, which was logged into using the default username and password of 'admin' and 'password'. For demonstration purposes, the security of the site was set to low.

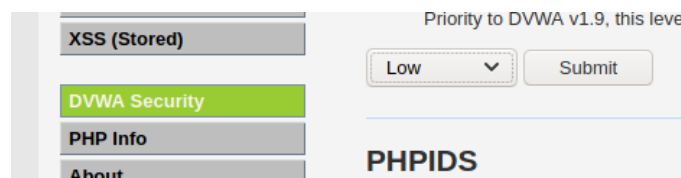


Figure 6. Setting the security to low.

The page SQL Injection was then selected from the left-hand menu bar.

Wireshark was then booted and Wlan0 was selected so that the program would read the traffic from the DVWA website.

On the SQL Injection page, the user ID of 1 was submitted which returned the first name of 'admin' and a surname of 'admin'.

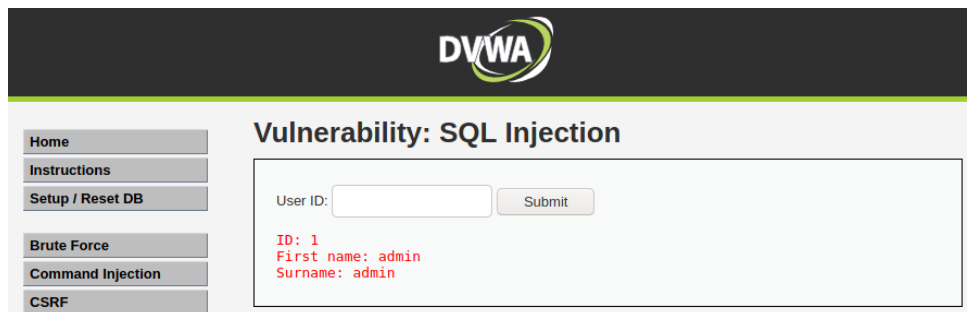


Figure 7. Submitting 1 on the SQL Injection page.

On Wireshark, the filter was set to http and the GET command with the submitted user ID was found. The contents of the protocol were then copied to a text file for use with sqlmap.

http					
No.	Time	Source	Destination	Protocol	Length Info
311	61.458479740	192.168.99.147	192.168.99.13	HTTP	598 GET /dvwa/dvwa/images/logo.png HTTP/1.1
312	61.465591105	192.168.99.13	192.168.99.147	HTTP	252 HTTP/1.1 304 Not Modified
329	89.508443393	192.168.99.147	192.168.99.13	HTTP	644 GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit&us
331	89.539825728	192.168.99.13	192.168.99.147	HTTP	518 HTTP/1.1 302 Found
333	89.551767672	192.168.99.147	192.168.99.13	HTTP	564 GET /dvwa/vulnerabilities/sqli/index.php HTTP/1.1
335	89.588036368	192.168.99.13	192.168.99.147	HTTP	507 HTTP/1.1 200 OK (text/html)
337	89.955571200	192.168.99.147	192.168.99.13	HTTP	570 GET /dvwa/dvwa/css/main.css HTTP/1.1
338	89.962451730	192.168.99.13	192.168.99.147	HTTP	274 HTTP/1.1 304 Not Modified
339	89.981487069	192.168.99.147	192.168.99.13	HTTP	557 GET /dvwa/dvwa/js/dvwaPage.js HTTP/1.1
340	89.984924886	192.168.99.13	192.168.99.147	HTTP	274 HTTP/1.1 304 Not Modified
342	90.045140907	192.168.99.147	192.168.99.13	HTTP	570 GET /dvwa/dvwa/images/logo.png HTTP/1.1
343	90.048256484	192.168.99.13	192.168.99.147	HTTP	252 HTTP/1.1 304 Not Modified
385	92.615671183	192.168.99.147	192.168.99.13	HTTP	636 GET /dvwa/vulnerabilities/sqli/index.php?id=1&Submit=
389	92.656274885	192.168.99.13	192.168.99.147	HTTP	506 HTTP/1.1 200 OK (text/html)
391	92.964674270	192.168.99.147	192.168.99.13	HTTP	607 GET /dvwa/dvwa/css/main.css HTTP/1.1
393	92.971785946	192.168.99.13	192.168.99.147	HTTP	274 HTTP/1.1 304 Not Modified
401	93.008898133	192.168.99.147	192.168.99.13	HTTP	594 GET /dvwa/dvwa/js/dvwaPage.js HTTP/1.1
402	93.012764857	192.168.99.13	192.168.99.147	HTTP	274 HTTP/1.1 304 Not Modified
Frame 385: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface wlan0, id 0					
Ethernet II, Src: Raspberr_71:de:ae (b8:27:eb:71:de:ae), Dst: Lifetron_09:6f:32 (00:0f:60:09:6f:32)					
Internet Protocol Version 4, Src: 192.168.99.147, Dst: 192.168.99.13					
Transmission Control Protocol, Src Port: 58454, Dst Port: 80, Seq: 2576, Ack: 2944, Len: 570					
Hypertext Transfer Protocol					
GET /dvwa/vulnerabilities/sqli/index.php?id=1&Submit=Submit&user_token=82f43b4f2f1c5f2f7c213a915058a0d8 HTTP/1.1\r\n					
Host: 192.168.99.13\r\n					
User-Agent: Mozilla/5.0 (X11; Linux armv7l; rv:78.0) Gecko/20100101 Firefox/78.0\r\n					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n					
Accept-Language: en-US,en;q=0.5\r\n					
Accept-Encoding: gzip, deflate\r\n					
Connection: keep-alive\r\n					
Referer: http://192.168.99.13/dvwa/vulnerabilities/sqli/index.php\r\n					
Cookie: security=impossible; security=low; PHPSESSID=vp2d4nlk7vic6b5r8t9kq5rp83\r\n					

Figure 8. Wireshark protocol analysis.

```
GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.99.13
User-Agent: Mozilla/5.0 (X11; Linux armv7l; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.99.13/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=3o0gld1lo91ek64cb2mvss9re4|
```

Figure 9. Creating the file for use with sqlmap.

The text file was saved on the desktop as dvwa.txt and the following command was run:

```
kali@kali:~$ sqlmap -r /home/kali/Desktop/dvwa.txt --dbms=MySQL -a --output-dir=/home/kali/Desktop --batch
```

Figure 10. sqlmap command.

The attempt was successful and the users table from the DVWA website was found.

user_id	avatar	user	password	last_name	first_name	last_login	failed_login
1	http://playground.raspwn.org/dvwa/hackable/users/admin.jpg	admin	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	#####	0
2	http://playground.raspwn.org/dvwa/hackable/users/gordonb.jpg	gordonb	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	#####	0
3	http://playground.raspwn.org/dvwa/hackable/users/1337.jpg	1337	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	#####	0
4	http://playground.raspwn.org/dvwa/hackable/users/pablo.jpg	pablo	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	#####	0
5	http://playground.raspwn.org/dvwa/hackable/users/smithy.jpg	smithy	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	#####	0

Figure 11. DVWA users table.

The scan was completed in 186 seconds.

#### 2.3.2.4 John the Ripper

Although sqlmap does crack the password hashes, John the Ripper was used to demonstrate how the tool can be used.

A text file was created using the 'username:hash' format to store the username and hashes from the user table discovered during the sqlmap attack.

```
admin:f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Figure 12. User password hash text file.

The command 'sudo john --format=raw-md5 /home/Kali/Desktop/userPasswords.txt' was used.

```
kali@kali:~$ sudo john --format=raw-md5 /home/kali/Desktop/userPasswords.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 32/32])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password      (smithy)
abc123         (gordonb)
letmein        (pablo)
Proceeding with incremental:ASCI
charley        (1337)
4g 0:00:00:02 DONE 3/3 (2021-05-16 15:38) 1.498g/s 67831p/s 67831c/s 71364C/s stevy13..chandog
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

Figure 13. John the Ripper cracking the passwords.

The format forces the program to recognize the hashes as MD5. The scan was completed in 2 seconds using the default wordlist.

Running the '-- show' command reveals all the cracked passwords:

```
kali@kali:~$ sudo john --show --format=raw-md5 /home/kali/Desktop/userPasswords.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Figure 14. Successfully cracked passwords.

## 2.4 STICKY FINGERS KALI-PI

### 2.4.1 Installation

Firstly, the Sticky Fingers Kali-Pi image was downloaded from the website.

The Raspberry Pi imager was then used to write the image to the Micro SD Card.

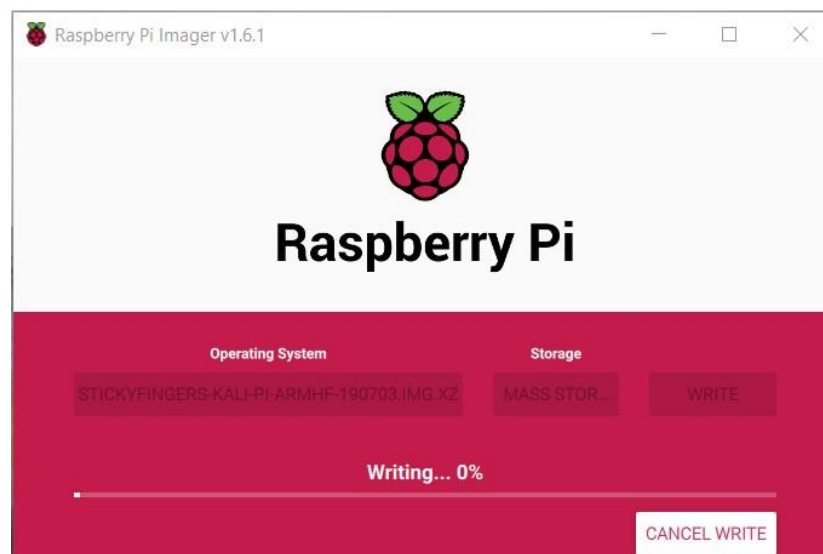


Figure 15. Using the Raspberry Pi imager to write the operating system to the SD card.

As Kali-Pi had been designed for touchscreens, the Pi was booted attached to the official Raspberry Pi 7" Touchscreen. Upon initial boot, the screen was upside down.

After logging in as user 'pi' with password 'raspberrypi', as per the instructions, the following command was run:

```
pi@kali-pi:~$ sudo kalipi-tft-config
```

Figure 16. sudo Kalipi-tft-config command

This opened the command line display configuration window where the display could be configured. The official Raspberry Pi touchscreen was selected, and the option was selected to rotate the screen 180 degrees.

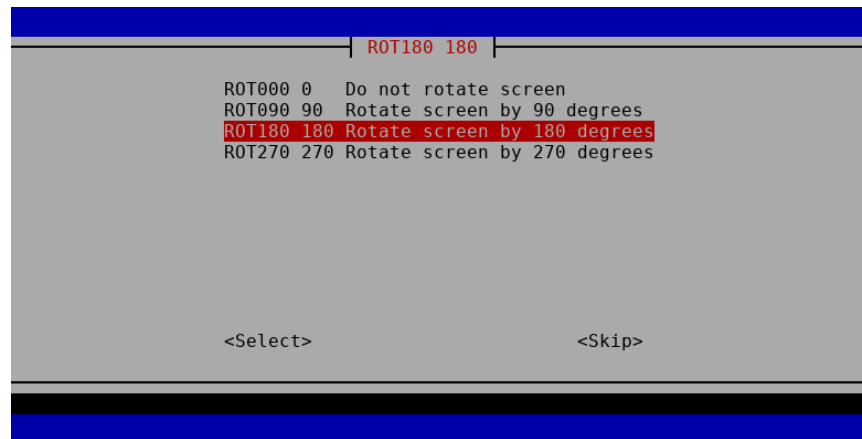


Figure 16. Fixing the Raspberry Pi screen issue.

After that the next config command was run:

```
pi@kali-pi:~$ sudo kalipi-config
```

Figure 18. sudo Kalipi-config command.

This opened the command line configuration window. The WiFi was initially configured to the home network rather than the vulnerable image in case any updates needed to be retrieved. Then the boot option was set to boot to the CLI and auto-login as 'pi' which was necessary to run the Sticky Fingers launcher which was the custom launcher for the touchscreen.

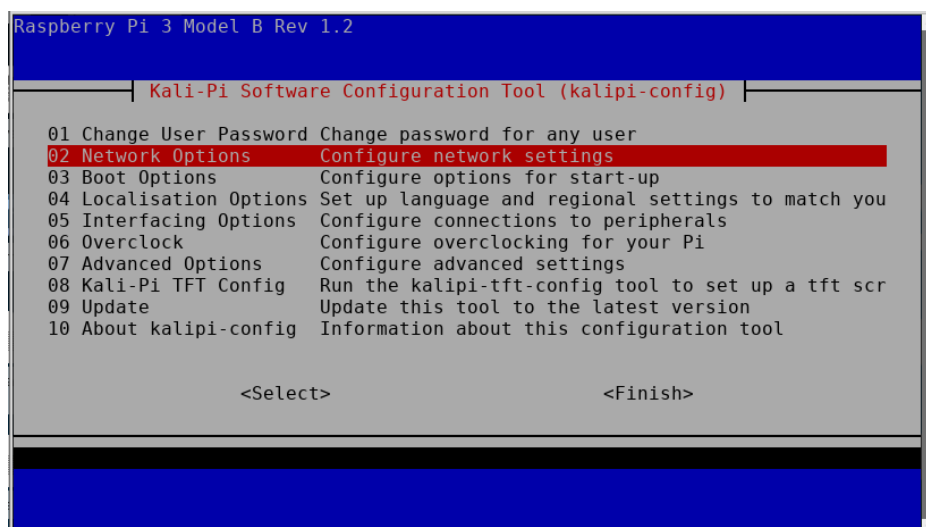


Figure 17. Kali-Pi Software Configuration Tool.

Due to the display not being filled by the screen, parts of the window were cut off and some guesswork was required as to what was being asked during the configuration progress.

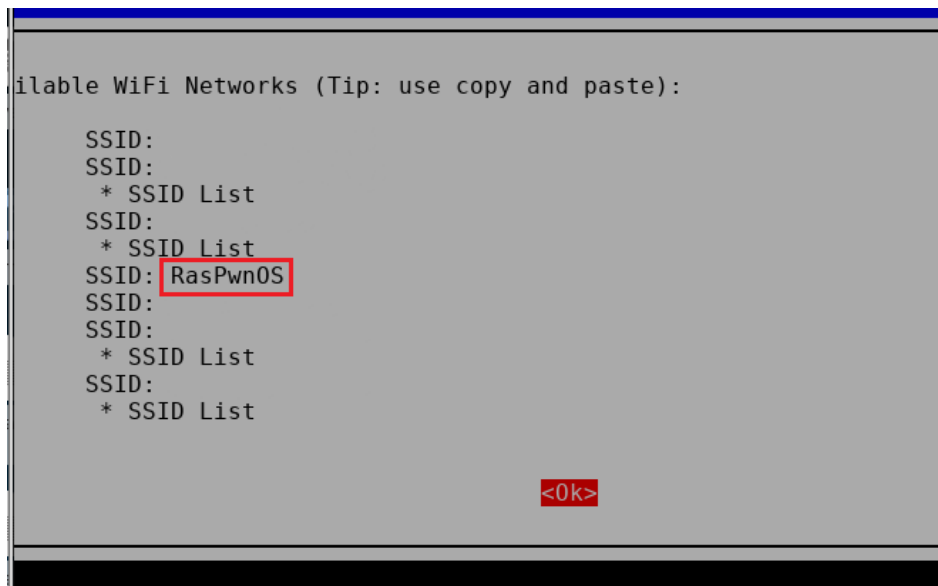


Figure 18. WiFi config screen. Some of the screen has been cut off.

Finally, the menu file located at 'home/pi/Kali-Pi' was changed to be set to the Raspberry Pi official touchscreen.

The Pi was then rebooted but displayed a black screen when trying to launch the Sticky Fingers interface.

After some troubleshooting, a forum post was found by the author stating that the launcher did not function with the Raspberry Pi Official Touchscreen. (Re4son, 2018)

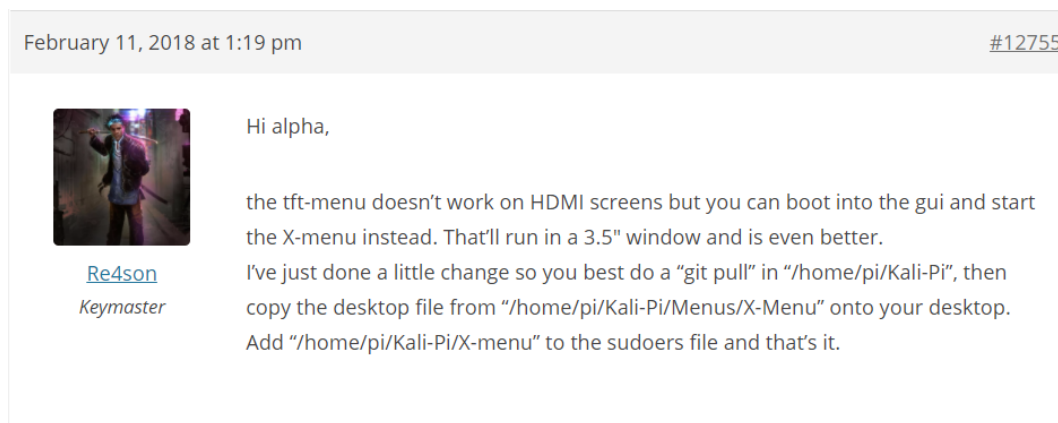


Figure 19. Forum post stating that the launcher won't work on the Raspberry Pi touch screen as it is classed as 'hdmi'

It was possible to run the launcher via the Kali desktop by opening the X-menu file, however, the only buttons that functioned were the arrow buttons to flick between screens. None of the other buttons worked.

Whilst this meant that the launcher could not be tested, the Kali desktop was still functioning and so this could be tested instead.

When trying to switch Wi-Fi connections to the RasPwn OS vulnerable Wi-Fi, the system did not recognize the change and continued to stay connected to the home network. After a few unsuccessful attempts, which included multiple reboots of the system, a fresh image was written to the SD card.

This then allowed the device to connect to the vulnerable server. This issue did not occur again, so its cause was unknown.

## 2.4.2 Tools Test

### 2.4.2.1 Nmap

Like Kali, an Nmap scan was run against 'playground.raspwn.org'.

```
pi@kali-pi:~$ nmap -v -A playground.raspwn.org
```

Figure 20. Kali-Pi nmap command.

The scan produced the same output as Kali, which can be found in Appendix C. The scan was completed in 97.17 seconds.

### 2.4.2.2 Nikto

The default installation of Kali-Pi did not come preinstalled with Nikto.

```
pi@kali-pi:~/Desktop$ sudo apt-get install nikto
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libfile-readbackwards-perl libssl-dev tigervnc-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  nikto
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 413 kB of archives.
After this operation, 2500 kB of additional disk space will be used.
Err:1 http://http.kali.org/kali kali-rolling/non-free armhf nikto all 1:2.1.6+git20190310-0kali2
      404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/non-free/n/nikto/nikto_2.1.6+git20190310-0kali2_all.deb 404 Not Found [IP: 192.99.200.113 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

Attempting to install the tool was unsuccessful and therefore the scan could not be tested.



### 2.4.2.3 Wireshark & sqlmap

As with Kali, sqlmap was used to launch an SQL injection brute force attack. On the DVWA, the security was set to low, and the admin user was retrieved from the database. During this time, the screenshot functionality was being temperamental, so images were taken where necessary.

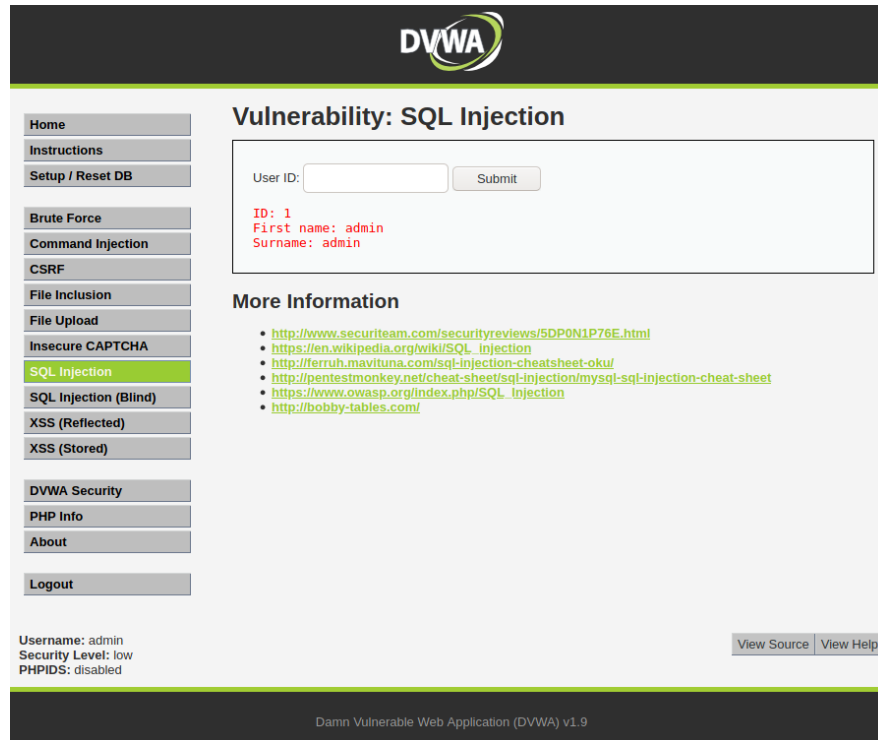


Figure 21. DVWA SQL Injection page.

Using Wireshark, a http filter was set up to retrieve the necessary protocol data. This was then added to a text file.

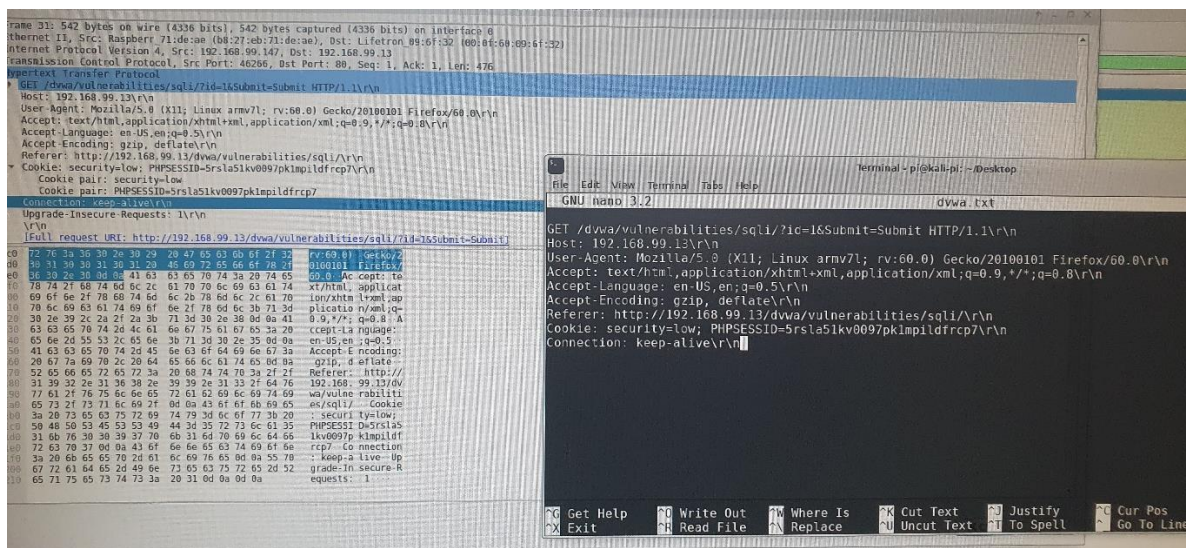


Figure 22. Wireshark protocol analysis and text file containing the necessary data.

The sqlmap command was then run as on Kali.

```
[*] starting @ 21:11:07 /2019-07-03/
[21:11:07] [INFO] parsing HTTP request from '/home/pi/Desktop/dvwa.txt'
[21:11:07] [WARNING] using '/home/pi/Desktop' as the output directory
[21:11:07] [INFO] testing connection to the target URL
[21:11:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:11:09] [INFO] testing if the target URL content is stable
[*] ending @ 21:15:28 /2019-07-03/
```

Figure 23. sqlmap command start and end time.

The scan completed in 261 seconds and successfully retrieved the user table.

#### 2.4.2.4 John the Ripper

The password hashes from the users database were added to a text file using the 'username:hash' format as before. The john command was then used which successfully cracked the passwords.

```
pi@kali-pi:~/Desktop$ sudo john --format=raw-md5 /home/pi/Desktop/userPasswords.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 32/32])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
charley (1337)
lg 0:00:00:02 DONE 3/3 (2021-05-17 01:23) 0.3861g/s 68942p/s 68942c/s 68942C/s stevy13..chandog
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
pi@kali-pi:~/Desktop$ sudo john --show --format=Raw-MD5 userPasswords.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Figure 24. John the Ripper cracked passwords.

This took a total of 2 seconds.

## 2.5 PwnPi

---

### 2.5.1 Installation

The image file zip was downloaded from the PwnPi website and then extracted using 7-Zip.



Figure 25. PwnPi download link.

The operating system was installed using the Raspberry Pi imager, by navigating to 'Use custom' in the Operating System menu and selecting the extracted image file.



Figure 26. Using the Raspberry Pi imager to write the operating system to the SD card.

Once the installation was completed, the SD card was inserted into the Raspberry Pi which was then powered on. Unfortunately, while the Raspberry Pi was receiving power it did not boot.

A potential fix found was to download the Raspberry Pi firmware and add the boot files to the boot folder on the SD card (Muniz & Lakhani, 2015). The firmware was downloaded as a ZIP folder from 'https://github.com/raspberrypi/firmware'.

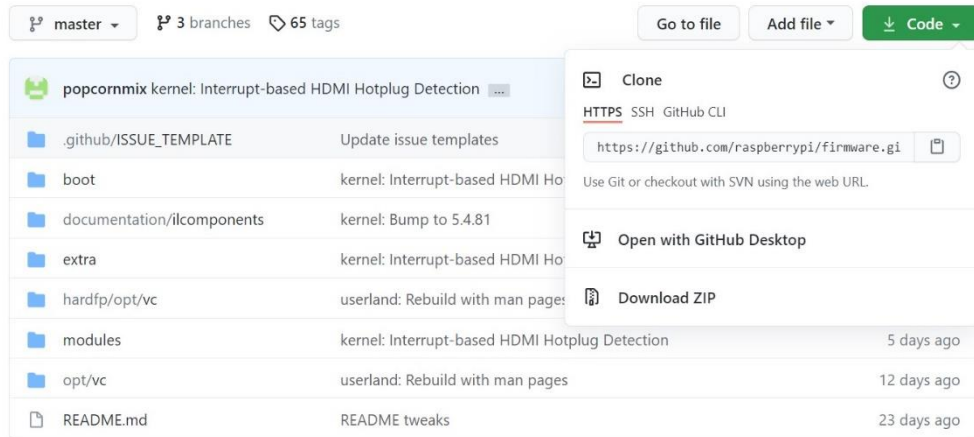


Figure 27. Raspberry Pi firmware GitHub repo.

Once downloaded, the files in the boot folder were then copied over to the boot folder on the SD card. This encountered another issue however in that the boot partition created by the imager was not big enough for all the firmware files.



Figure 28. Screenshot showing the partition as only 56 MB.

As the SD card had been formatted using FAT, it was not possible to extend the partition using the built-in windows disk management tool and therefore a third-party tool had to be installed (Microsoft, 2021).

The program MiniTool Partition Wizard, which is a partition manager built for Windows (MiniTool Software Limited, 2021), was downloaded and then used to extend the primary partition by approximately 500MB. This then allowed for the firmware files to be copied over.



Figure 29. MiniTool Partition Wizard extending the partition.





Figure 30. Screenshot showing new larger partition size.

The SD card was then plugged into the Raspberry Pi and the Pi successfully booted.



Figure 31. Initial command line interface when first booting PwnPi.

When logged in, the command ‘startx’ needs to be run to boot the GUI.

## 2.5.2 Tools Test

### 2.5.2.1 Nmap

As done previously, an Nmap scan was attempted against ‘playground.raspwn.org’. However, the scan was unsuccessful as it kept returning that the RasPwn Host was down despite that being incorrect.

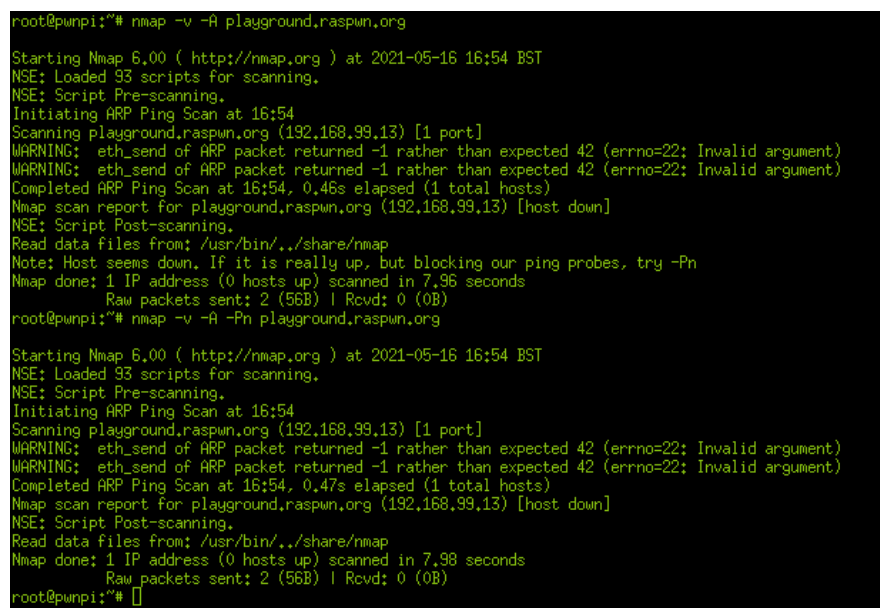


Figure 32. Screenshot showing unsuccessful Nmap scan.

### 2.5.2.2 Nikto

A Nikto scan was also run against 'playground.raspwn.org'. Fortunately, this was successful however it did not discover as many issues as the previous two scans. Presumably, this was because the version was older.

```
root@pwnpi:~# nikto -h playground.raspwn.org
- Nikto v2.1.4

+-----+
+ Target IP:      192.168.99.13
+ Target Hostname: playground.raspwn.org
+ Target Port:    80
+ Start Time:     2021-05-17 16:56:58
+-----+

+ Server: Apache/2.2.22 (Debian)
+ Retrieved x-powered-by header: PHP/5.4.36-0+deb7u1
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ DEBUG: HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-240: /scripts/usa.dll/USServiceanything?USMAdmin: Allows Webspeed to be remotely administered, Edit unbroker.properties and set AllowMsngrCmds to 0.
+ OSVDB-12184: /index.php?PHPBB85F2A0-3C92-11d5-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3233: /icons/README: Apache default file found.
- STATUS: Completed 4280 tests ("66% complete, 16.2 minutes left: currently in plugin 'Nikto Tests')
- STATUS: Completed 6020 tests ("93% complete, 3.1 minutes left: currently in plugin 'Nikto Tests')
+ 6448 items checked: 9 error(s) and 6 item(s) reported on remote host
+ End Time:      2021-05-17 17:41:25 (2667 seconds)
+-----+

+ 1 host(s) tested
root@pwnpi:~#
```

Figure 33. Nikto scan.

The scan was completed in 2667 seconds.

### 2.5.2.3 Wireshark & sqlmap

The command Wireshark was issued via the terminal to start the Wireshark gui as this was not possible from the right click menu.

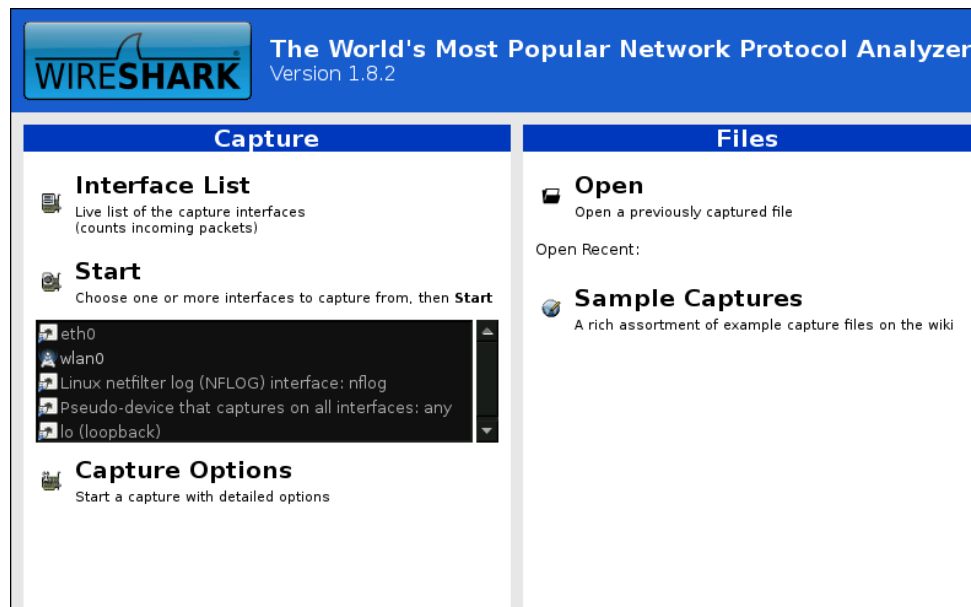


Figure 34. Wireshark GUI.

Wlan0 was selected to capture from, and the http filter was added. On the DVWA website, the security was set to low and the user ID of 1 was submitted.

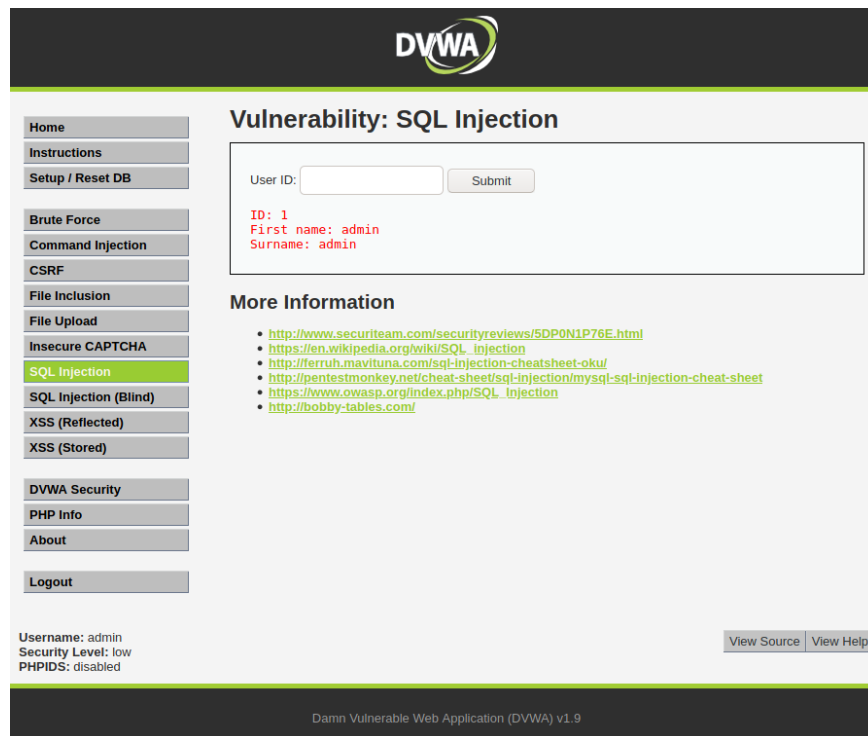


Figure 35. Getting the admin user from the database.

On Wireshark, the packet information was used to generate the request file to be used by sqlmap.

```
1 GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: 192.168.99.13
3 User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-gb) AppleWebKit/535+ (KHTML, like Gecko) Version/5.0 Safari/535.22+ Midori/0.4
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Referer: http://192.168.99.13/dvwa/vulnerabilities/sqli/
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-gb;q=0.750
8 Connection: Keep-Alive
9 Cookie: security=low; PHPSESSID=3boft9qlq2bdrjrp0nuvj358fd
```

Figure 36. sqlmap request file.

Whilst the Wireshark version used was outdated it did work successfully. The built-in web browser though was extremely slow, and it took a few minutes for each web page to load.

Initially trying to run sqlmap as described previously was unsuccessful. Eventually, after some troubleshooting, it was found that the command used had to be 'python sqlmap.py ...' and it needed to be run from the /pentest/database/sqlmap-dev folder.

```

sqlmap/1.0-dev-f305dde - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, s

[*] starting at 18:09:48

[18:09:48] [INFO] parsing HTTP request from '/root/dvwa.txt'
[18:09:48] [INFO] testing connection to the target url
[18:09:48] [INFO] testing if the url is stable, wait a few seconds
[18:09:50] [INFO] url is stable
[18:09:50] [INFO] testing if GET parameter 'id' is dynamic
[18:09:50] [WARNING] GET parameter 'id' does not appear dynamic
[18:09:50] [INFO] heuristics detected web page charset 'ascii'
[18:09:50] [WARNING] reflective value(s) found and filtering out
[18:09:50] [INFO] heuristic test shows that GET parameter 'id' might be injectable (possible DBMS: MySQL)
[18:09:50] [INFO] testing for SQL injection on GET parameter 'id'
[18:09:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:09:51] [INFO] GET parameter 'id' seems to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='Surname: admin')
[18:09:51] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[18:09:51] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause' injectable
[18:09:51] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[18:09:51] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'

[18:11:53] [INFO] table 'information_schema.VIEWS' dumped to CSV file '/pentest/database/sqlmap-dev/output/192.168.99.13/dump/information_schema/VIEWS.csv'
[18:11:53] [INFO] fetched data logged to text files under '/root/.192.168.99.13'

[*] shutting down at 18:11:53

root@pwnpi:/pentest/database/sqlmap-dev#

```

Figure 37. sqlmap attack screenshots.

The scan itself however was successful and retrieved the users table along with the hashed passwords. The scan completed in 125 seconds.

#### 2.5.2.4 John the Ripper

Unfortunately, trying to run John the Ripper to crack the password hashes was also unsuccessful. The program would not crack the hashes despite multiple attempts.

```

root@pwnpi:/etc/john# john --wordlist=/usr/share/john/password.lst /root/userPasswords.txt
Loaded 8 password hashes with no different salts (LM DES [32/32 BS])
guesses: 0 time: 0:00:00:00 100% c/s: 839200 trying: 222222 - HALLO
root@pwnpi:/etc/john#

```

Figure 38. Unsuccessful John the Ripper attempt.



# 3 RESULTS

## 3.1 REVIEW FACTOR SCORES

---

To review the operating systems described in this paper, a numbering system was implemented to grade each operating system on selected features. The system used a grade of 1-5, with 1 being the lowest score and 5 being the highest. Details on how each score was valued can be found in the grading rubrics in Appendix D.

When selecting the specific factors to review, the focus was placed on perceived beginner friendliness.

The tools were graded on the following:

1. Ease of Installation
2. Documentation available
3. Ease of use
4. Tools Built In

### 3.1.1 Kali Linux

*Table 1 - Kali Linux Review Scores.*

<b>Review Factor</b>	<b>Score</b>
<i>Ease of Installation</i>	4
<i>Documentation</i>	5
<i>Ease of Use</i>	5
<i>Tools Available</i>	5
<b>Total</b>	<b>19</b>

### 3.1.2 Sticky Fingers Kali-Pi

*Table 2 - Sticky Fingers Kali-Pi Review Scores.*

<b>Review Factor</b>	<b>Score</b>
<i>Ease of Installation</i>	4
<i>Documentation</i>	4
<i>Ease of Use</i>	4
<i>Tools Available</i>	4
<b>Total</b>	<b>16</b>

### 3.1.3 PwnPi

Table 3 - PwnPi Review Scores.

Review Factor	Score
Ease of Installation	2
Documentation	2
Ease of Use	2
Tools Available	3
<b>Total</b>	<b>9</b>

### 3.1.4 Overall

#### Review Ratings

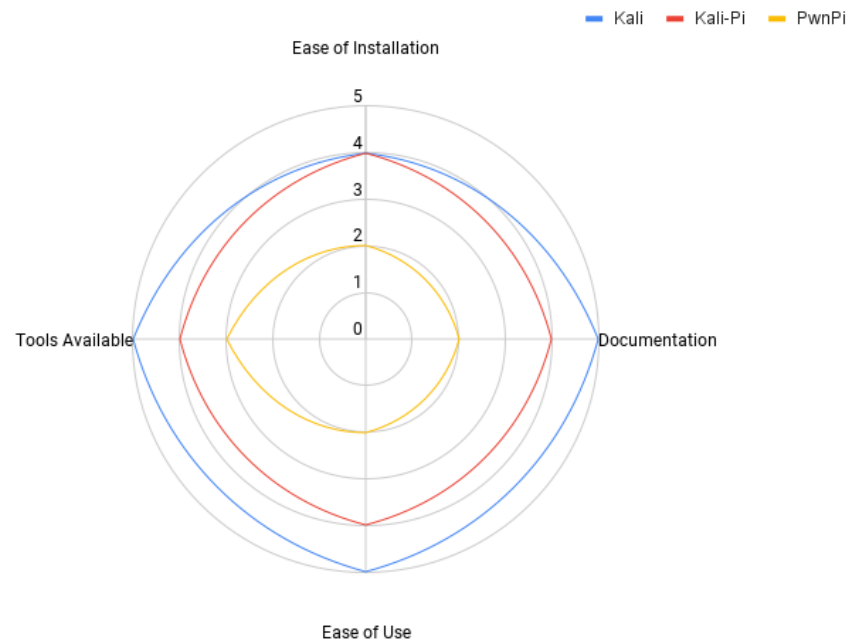


Figure 39. Review ratings radar chart.

Kali Linux for the Raspberry Pi scored the highest in Documentation, Ease of Use and Tools Available, as well as being joint highest for Ease of Installation.

Kali-Pi scored 4's across the board and was not last in any category.

PwnPi was the worst scoring operating system and came last in all four review factors.

## 3.2 SCAN TIMES COMPARISON

---

### 3.2.1 Nmap Scan

Total Time Taken for 'nmap' Scan

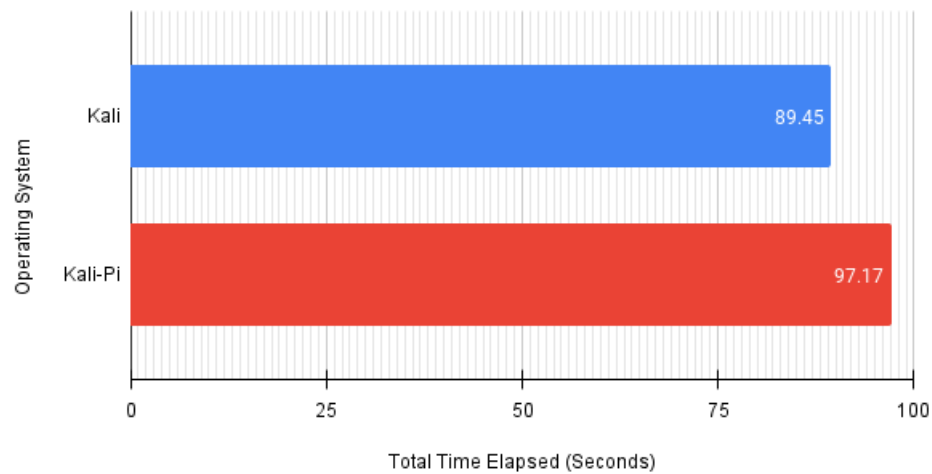


Figure 40. Total time taken for nmap scan.

The Nmap scan, unfortunately, did not work on PwnPi and so a comparison could only be drawn between Kali and Kali-Pi. Overall, the time taken was similar, but it ran slightly faster on the Kali Linux OS.

### 3.2.2 Nikto Scan

Total Time Taken for 'Nikto' Scan

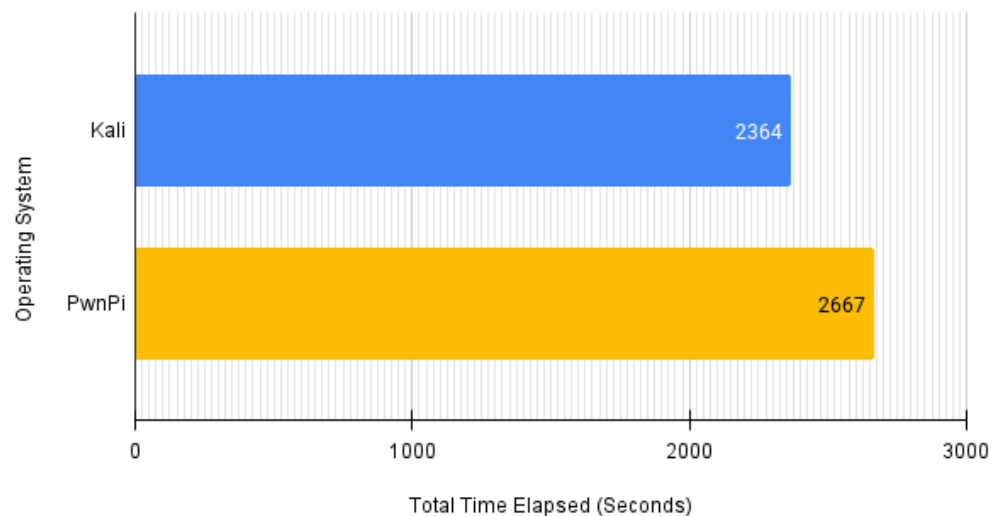


Figure 41. Total time taken for Nikto scan

Again, the Nikto scan did not work on all operating systems so a comparison could only be drawn from Kali and PwnPi. There was approximately a 5-minute difference between the two and the scan ran significantly faster on Kali.

### 3.2.3 sqlmap Scan

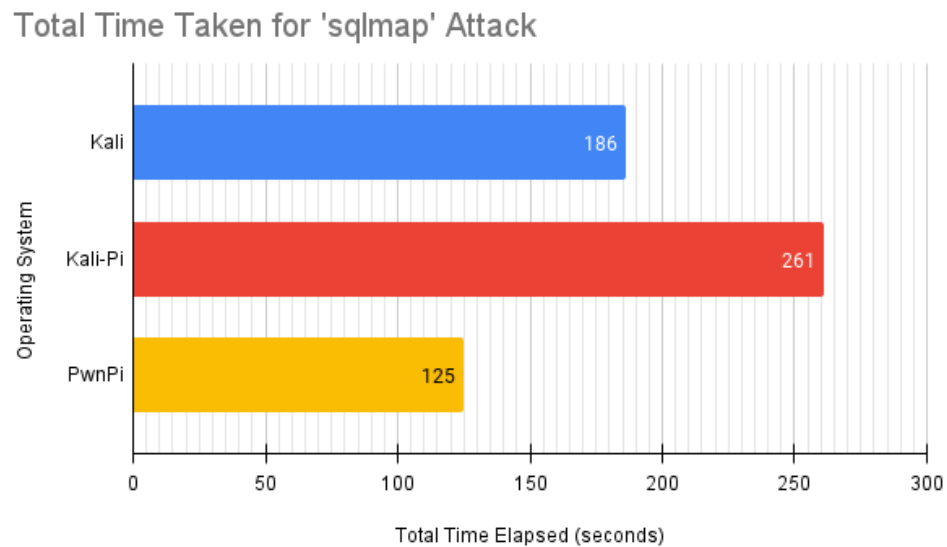


Figure 42. Total time taken for sqlmap attack.

During the sqlmap SQL injection brute force attack, Kali-Pi took the longest at 261 seconds, and PwnPi was the fastest at 125 seconds.

### 3.2.4 John the Ripper

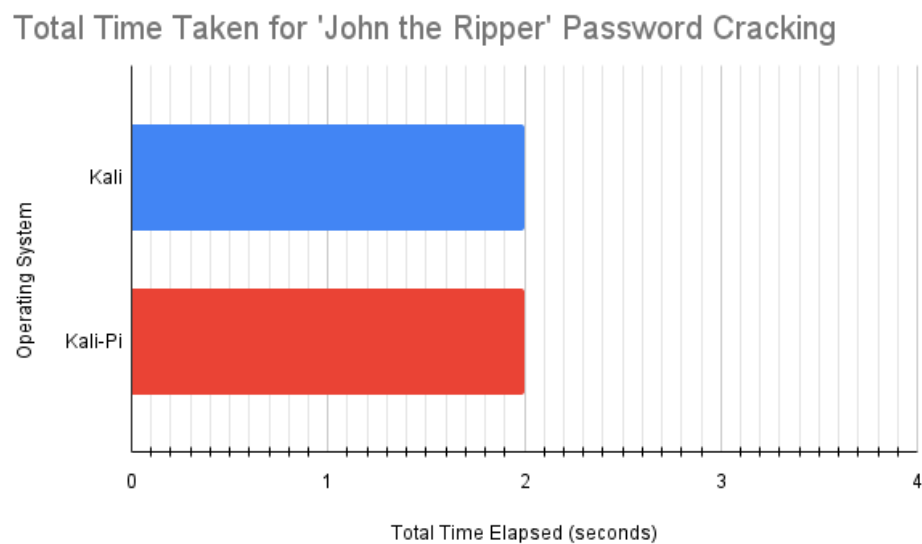


Figure 43. Total time taken for John the Ripper password cracking.

John the Ripper took 2 seconds to crack the found passwords on both Kali and Kali-Pi.

# 4 DISCUSSION

## 4.1 GENERAL DISCUSSION

---

### 4.1.1 Review Factor Scores

#### 4.1.1.1 *Kali Linux*

The Kali Linux distribution for the Raspberry Pi scored full marks in all the review factors bar ease of installation. Installation was simple and the Pi booted first try, however it was given a score of 4 as there was no documentation found indicating the login user and password. Trial and error discovered it to be 'Kali' and 'password' however this was inconsistent with its other distributions.

As Kali Linux is a popular operating system that can be used on a variety of devices, the documentation available is extensive and there is a large community present. Therefore, it scored 5/5 for documentation.

Full marks were given for ease of use as Kali looks and behaves like many other Linux distributions and has many similarities to Windows/macOS. Therefore, users who have used Linux before will face no issues and those who have not will find the transition natural.

In terms of tools available, Kali Linux came with an extensive pen-testing suite and all tools tested worked as expected, so full marks were awarded.

There were a few occasions when a temperature warning was given whilst using Kali Linux on the Raspberry Pi. Potential countermeasures to this may include buying a heatsink for the Pi. These can be purchased for as little as £2 and so is not a major issue. Such problems may not occur on newer versions of the Raspberry Pi like the 4 series which is available with up to 8GB of RAM. Unfortunately, this was not tested in the whitepaper and so cannot be confirmed.

One noted aspect of this operating system is that a minimum SD card size of 16GB is required.

#### 4.1.1.2 *Sticky Fingers Kali-Pi*

Sticky Fingers Kali-Pi scored well in all review factors. Ease of installation was given a 4/5. Although issues were faced, this was down to the hardware available during the research as opposed to the operating system itself. Booting into the desktop GUI was simple and worked the first time. A point was deducted as although it is stated that the Sticky Fingers launcher does not work with the Official Raspberry Pi 7" touchscreen, this information was hidden in the forum and not accessible.

Documentation was given a 4/5 as the installation instructions are written along with further documentation and tips. A point was deducted as a lot of information is also present within the forums which is not easy to navigate.

Ease of use was given a 4/5. The desktop GUI is very similar to the official Kali Linux's but has some differences. One major one was that there was no built-in text editor and so all files had to be opened in the command line which whilst still functional was inconvenient.

Tools available were given a 4/5. The basic installation of Kali-Pi came with a good number of tools but was missing some in comparison with the official Kali version. Only one point was deducted however as the full Kali-suite can be installed manually if need be. This does require a minimum of 16GB SD card, but 32GB is recommended. It also requires the file system to be extended manually.

#### **4.1.1.3 PwnPi**

PwnPi scored poorly in most review factors. A 2 was given for Ease of installation as the firmware had to be added and the partition extended to be able to boot in the first place. As there was no information outlining this a 2 was given for documentation. This was also given as there was no official documentation at all and the operating system is old and so lacks an active community.

A 2 was given for ease of use as the operating system uses OpenBox to manage windows. Whilst this works well, it is a lot different to major operating systems and even Linux distributions and so may not be intuitive for beginners. Many programs were located in different places than in Kali Linux and Kali-Pi so some trial and error was needed to find the right location to be able to run these programs. Especially as any command line programs selected through the GUI menu did not work.

A 3 was given for tools available as although the list was extensive, many were outdated or did not work.

#### **4.1.2 Scan Times**

The Kali operating system performed consistently. It was the fastest of the Nmap and Nikto scans and performed the same as Kali-Pi when it came to John the Ripper. The only thing it wasn't fastest at was sqlmap, but it was still faster than Kali-Pi.

Kali-Pi performed well but was slower than Kali when it came to the Nmap scan and was the slowest in the sqlmap attack.

PwnPi had inconsistent results. It was significantly slower than Kali when it came to the Nikto scan but was by far the fastest at the SQL Injection attack. Unfortunately, both the Nmap and John the Ripper tools did not work and therefore limited conclusions can be drawn.

## **4.2 CONCLUSIONS**

---

Kali Linux performed consistently well in scans and scored the highest in the review factors. Out of those tested, Kali Linux is the best penetration testing operating system for the Raspberry Pi, particularly for beginners to ethical hacking.

Kali-Pi scored well and using the vanilla Desktop GUI would be a good alternative, especially if the full Kali-suite were downloaded. This does however require a larger SD card.

Although PwnPi was the worst scoring, it did outperform in the sqlmap attack and does offer a wide variety of tools. It was let down by the fact that the operating system is no longer maintained and so has little documentation, all tools were outdated, and some did not work. Had it been a newer/maintained version, it would likely have scored much higher.

## 4.3 FUTURE WORK

---

Unfortunately, not all the tools tested in this research worked on every operating system, making it more difficult to compare the three. In future, a wider variety of tools could have been tested so that even if some did not work, there would still be plenty of data to draw conclusions from.

It was not until research had already started that it was discovered that the touchscreen being used was not compatible with the Sticky Fingers Kali-Pi launcher. In future, a compatible touchscreen would be used to allow for a more thorough review. This would also mean that all three operating systems would have been much different, as opposed to two very similar Kali desktop GUIs being reviewed alongside PwnPi.

Grading rubrics have been used to keep the review factor scoring as objective as possible, but future research could include a survey or study to understand the opinions of a large group of individuals. This could include taking a group of people who are new to penetration testing, asking them to carry out similar tasks as described in this paper and giving their own review scores.

# REFERENCES

(ISC)<sup>2</sup>, 2020. *Cybersecurity Professionals Stand Up to a Pandemic: (ISC)<sup>2</sup> Cybersecurity Workforce Study, 2020*, s.l.: (ISC)<sup>2</sup>.

Franceschi-Bicchierai, L., 2019. 'Pwnagotchi' Is the Open Source Handheld That Eats Wi-Fi Handshakes. [Online]

Available at: <https://www.vice.com/en/article/xwekw4/pwnagotchi-is-the-open-source-handheld-that-eats-wi-fi-handshakes>

[Accessed 13 May 2021].

Guimaraes, B. & Stampar, M., 2021. *sqlmap*. [Online]

Available at: <https://sqlmap.org/>

[Accessed 17 May 2021].

Kali Linux, n.d. [Online]

Available at: <https://www.kali.org/>

[Accessed 14 May 2021].

Kali Linux, n.d. *Raspberry Pi 3*. [Online]

Available at: <https://www.kali.org/docs/arm/raspberry-pi-3/>

[Accessed 14 May 2021].

Kali Tools, 2014. *Nikto*. [Online]

Available at: <https://tools.kali.org/information-gathering/nikto>

[Accessed 17 May 2021].

Microsoft, 2021. *Extend a basic volume*. [Online]

Available at: <https://docs.microsoft.com/en-us/windows-server/storage/disk-management/extend-a-basic-volume>

[Accessed 12 May 2021].

MiniTool Software Limited, 2021. *MiniTool Partition Wizards Free 12.3*. [Online]

Available at: <https://www.partitionwizard.com/free-partition-manager.html>

[Accessed 17 May 2021].

Muniz, J. & Lakhani, A., 2015. *Penetration Testing with Raspberry Pi*. Birmingham: Packt Publishing Ltd..

Nmap, n.d. *Nmap*. [Online]

Available at: <https://nmap.org/>

[Accessed 17 May 2021].

openwall, n.d. *John the Ripper password cracker*. [Online]

Available at: <https://www.openwall.com/john/>

[Accessed 17 May 2021].



PwnPi, n.d. *PWNPI.NET The Pen Test Drop Box Distro for the Raspberry Pi*. [Online]  
Available at: <http://pwnpi.sourceforge.net/index.html>  
[Accessed 12 May 2021].

Raspberry Pi Foundation, 2020. *Raspberry Pi Foundation Review*, s.l.: Raspberry Pi.

Raspberry Pi Foundation, n.d. *Raspberry Pi Foundation Strategy 2018-2020*. [Online]  
Available at:  
<https://static.raspberrypi.org/files/about/RaspberryPiFoundationStrategy2018%E2%80%932020.pdf>  
[Accessed 17 May 2021].

Raspberry Pi Foundation, n.d. *What is a Raspberry Pi*. [Online]  
Available at: <https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/>  
[Accessed 13 May 2021].

Raspberry Pi, n.d. *Raspberry Pi Imager*. [Online]  
Available at: <https://www.raspberrypi.org/software/>  
[Accessed 14 May 2021].

RasPwn OS, 2016. *RasPwn OS*. [Online]  
Available at: <http://raspwn.org/>  
[Accessed 14 May 2021].

Re4son, 2018. *Problem with 7" pi screen - no button menu*. [Online]  
Available at: <https://whitedome.com.au/re4son/topic/problem-with-7-pi-screen-no-button-menu/>  
[Accessed 14 May 2021].

Re4son, 2018. *Sticky Fingers Kali-Pi*. [Online]  
Available at: <https://whitedome.com.au/re4son/sticky-fingers-kali-pi/>  
[Accessed 14 May 2021].

Stack Overflow, 2020. *2020 Developer Survey*. [Online]  
Available at: <https://insights.stackoverflow.com/survey/2020#technology-most-loved-dreaded-and-wanted-platforms-wanted5>  
[Accessed 13 May 2021].

VMware, Inc., 2020. *Global Threat Report*, Palo Alto: s.n.

Wireshark Foundation, n.d. [Online]  
Available at: <https://www.wireshark.org/#download>  
[Accessed 17 May 2021].

# APPENDICES

## APPENDIX A – KALI LINUX NMAP SCAN

---

```
nmap -v -A playground.raspwn.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 21:35 UTC
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:35
Completed NSE at 21:35, 0.00s elapsed
Initiating NSE at 21:35
Completed NSE at 21:35, 0.00s elapsed
Initiating NSE at 21:35
Completed NSE at 21:35, 0.00s elapsed
Initiating Ping Scan at 21:35
Scanning playground.raspwn.org (192.168.99.13) [2 ports]
Completed Ping Scan at 21:35, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:35
Completed Parallel DNS resolution of 1 host. at 21:35, 0.00s elapsed
Initiating Connect Scan at 21:35
Scanning playground.raspwn.org (192.168.99.13) [1000 ports]
Discovered open port 80/tcp on 192.168.99.13
Discovered open port 443/tcp on 192.168.99.13
Discovered open port 139/tcp on 192.168.99.13
Discovered open port 8080/tcp on 192.168.99.13
Discovered open port 22/tcp on 192.168.99.13
Discovered open port 445/tcp on 192.168.99.13
Discovered open port 5001/tcp on 192.168.99.13
Discovered open port 901/tcp on 192.168.99.13
Completed Connect Scan at 21:35, 0.43s elapsed (1000 total ports)
Initiating Service scan at 21:35
Scanning 8 services on playground.raspwn.org (192.168.99.13)
Completed Service scan at 21:36, 11.04s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.99.13.
Initiating NSE at 21:36
Completed NSE at 21:37, 72.96s elapsed
Initiating NSE at 21:37
Completed NSE at 21:37, 1.70s elapsed
Initiating NSE at 21:37
Completed NSE at 21:37, 0.01s elapsed
Nmap scan report for playground.raspwn.org (192.168.99.13)
Host is up (0.032s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
|_ ssh-hostkey:
|   1024 2d:df:2d:f8:3a:b5:c3:95:9f:bf:0b:ac:92:07:c9:fb (DSA)
|   2048 fe:6c:d7:fc:d8:3c:1f:df:23:e9:27:c0:d9:47:58:c5 (RSA)
|_  256 24:33:64:6f:ac:0c:9e:60:5d:bc:d9:e0:53:b8:52:f9 (ECDSA)
80/tcp    open  http         Apache httpd 2.2.22 ((Debian))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Welcome to the Playground! | RasPwn Web Playground
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/https?
|_   ssl-cert: Subject: commonName=charon.us/organizationName=Ferryman
Services/stateOrProvinceName=CO/countryName=US
|_   Issuer: commonName=charon.us/organizationName=Ferryman
Services/stateOrProvinceName=CO/countryName=US
```

```

| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-04-01T12:04:05
| Not valid after: 2018-04-01T12:04:05
| MD5: 42d4 6ce2 9a8d 8309 87cc 88d0 3d2b ca9f
|_SHA-1: 5f24 d87a 50f9 5a5a 1321 8e54 a862 618e f51d b586
|_ssl-date: 2016-09-04T23:23:31+00:00; -4y249d22h13m45s from scanner time.
445/tcp open netbios-ssn Samba smbd 3.6.6 (workgroup: WORKGROUP)
901/tcp open http Samba SWAT administration server
| http-auth:
| HTTP/1.0 401 Authorization Required\x0D
|_ Basic realm=SWAT
| http-methods:
|_ Supported Methods: GET POST
|_ http-title: 401 Authorization Required
5001/tcp open java-object Java Object Serialization
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Site doesn't have a title.
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.91%I=7%D=5/12%Time=609C4A3C%P=arm-unknown-linux-gnueab
SF:ihf%r(NULL,4,"\xac\xed\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1710d22h13m44s, deviation: 0s, median: -1710d22h13m45s
| nbstat: NetBIOS name: RASPNW, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| RASPNW<00> Flags: <unique><active>
| RASPNW<03> Flags: <unique><active>
| RASPNW<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
|_ WORKGROUP<00> Flags: <group><active>
| smb-os-discovery:
| OS: Unix (Samba 3.6.6)
| Computer name: raspwn
| NetBIOS computer name:
| Domain name:
| FQDN: raspwn
|_ System time: 2016-09-04T23:22:17+00:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

NSE: Script Post-scanning.
Initiating NSE at 21:37
Completed NSE at 21:37, 0.00s elapsed
Initiating NSE at 21:37
Completed NSE at 21:37, 0.00s elapsed
Initiating NSE at 21:37
Completed NSE at 21:37, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.45 seconds

```

## APPENDIX B – KALI LINUX NIKTO SCAN

---

```
nikto -h playground.raspwn.org
- Nikto v2.1.6
-----
+ Target IP:          192.168.99.13
+ Target Hostname:    playground.raspwn.org
+ Target Port:        80
+ Start Time:         2021-05-12 21:40:22 (GMT0)
-----
+ Server: Apache/2.2.22 (Debian)
+ Retrieved x-powered-by header: PHP/5.4.36-0+deb7u1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache
2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false
positives.
+ Uncommon header 'union all select filetoclob('/etc/passwd','server')' found, with
contents: :html,0 FROM sysusers WHERE username=USER --/.html HTTP/1.1 404 Not Found
+ Uncommon header 'src=javascript' found, with contents: alert('Vulnerable')><Img
Src=\" HTTP/1.1 404 Not Found
+ OSVDB-240: /scripts/wsisa.dll/WService=anything?WSMadmin: Allows Webspeed to be
remotely administered. Edit unbroke.properties and set AllowMsgnrCmds to 0.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
- STATUS: Completed 2990 requests (~43% complete, 19.4 minutes left): currently in
plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.30022 sec, 10 requests: 0.3016 sec.
+ Server may leak inodes via ETags, header found with file /icons/README, inode:
68627, size: 5108, mtime: Tue Aug 28 10:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
- STATUS: Completed 4260 requests (~62% complete, 13.2 minutes left): currently in
plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.29650 sec, 10 requests: 0.2933 sec.
- STATUS: Completed 5170 requests (~75% complete, 8.7 minutes left): currently in
plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.33281 sec, 10 requests: 0.3303 sec.
- STATUS: Completed 5930 requests (~86% complete, 4.9 minutes left): currently in
plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.28978 sec, 10 requests: 0.2907 sec.
+ Uncommon header '-al&absolute_path_studip=http' found, with contents:
//cirt.net/rfiinc.txt?? HTTP/1.1 404 Not Found
+ Uncommon header '-al&_phplib[libdir]=http' found, with contents:
//cirt.net/rfiinc.txt?? HTTP/1.1 404 Not Found
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL
databases, and should be protected or limited to authorized hosts.
+ 8018 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:          2021-05-12 22:19:46 (GMT0) (2364 seconds)
-----
+ 1 host(s) tested
```

## APPENDIX C – STICKY FINGERS KALI-PI NMAP SCAN

---

```
nmap -v -A playground.raspwn.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-03 20:18 AEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:18
Completed NSE at 20:18, 0.00s elapsed
Initiating NSE at 20:18
Completed NSE at 20:18, 0.00s elapsed
Initiating Ping Scan at 20:18
Scanning playground.raspwn.org (192.168.99.13) [2 ports]
Completed Ping Scan at 20:18, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:18
Completed Parallel DNS resolution of 1 host. at 20:18, 0.00s elapsed
Initiating Connect Scan at 20:18
Scanning playground.raspwn.org (192.168.99.13) [1000 ports]
Discovered open port 443/tcp on 192.168.99.13
Discovered open port 80/tcp on 192.168.99.13
Discovered open port 139/tcp on 192.168.99.13
Discovered open port 8080/tcp on 192.168.99.13
Discovered open port 445/tcp on 192.168.99.13
Discovered open port 22/tcp on 192.168.99.13
Discovered open port 901/tcp on 192.168.99.13
Discovered open port 5001/tcp on 192.168.99.13
Completed Connect Scan at 20:18, 0.43s elapsed (1000 total ports)
Initiating Service scan at 20:18
Scanning 8 services on playground.raspwn.org (192.168.99.13)
Completed Service scan at 20:18, 14.10s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.99.13.
Initiating NSE at 20:18
Completed NSE at 20:19, 74.31s elapsed
Initiating NSE at 20:19
Completed NSE at 20:19, 0.08s elapsed
Nmap scan report for playground.raspwn.org (192.168.99.13)
Host is up (0.037s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
|_ ssh-hostkey:
|   1024 22:df:2d:f8:3a:b5:c3:95:9f:bf:0b:ac:92:07:c9:fb (DSA)
|   2048 fe:6c:d7:fc:d8:3c:1f:df:23:e9:27:c0:d9:47:58:c5 (RSA)
|_  256 24:33:64:6f:ac:0c:9e:60:5d:bc:d9:e0:53:b8:52:f9 (ECDSA)
80/tcp    open  http         Apache httpd 2.2.22 ((Debian))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Welcome to the Playground! | RasPwn Web Playground
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/https?
|_ ssl-date: 2016-09-05T00:15:26+00:00; -2y301d10h03m26s from scanner time.
445/tcp   open  netbios-ssn Samba smbd 3.6.6 (workgroup: WORKGROUP)
901/tcp   open  http         Samba SWAT administration server
|_ http-auth:
|_   HTTP/1.0 401 Authorization Required\x0D
|_   Basic realm=SWAT
|_ http-methods:
|_   Supported Methods: GET POST
|_ http-title: 401 Authorization Required
5001/tcp  open  java-rmi     Java RMI
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
|_ http-server-header: Apache-Coyote/1.1
```

```

|_http-title: Site doesn't have a title.
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.70%I=7%D=7/3%Time=5D1C80FC%P=arm-unknown-linux-gnueabi
SF:hf%r(NULL,4,"\xac\xed\0\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1031d10h03m25s, deviation: 0s, median: -1031d10h03m26s
|_nbstat: NetBIOS name: RASPN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
|_Names:
|   RASPN<00>           Flags: <unique><active>
|   RASPN<03>           Flags: <unique><active>
|   RASPN<20>           Flags: <unique><active>
|   \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
|_  WORKGROUP<00>       Flags: <group><active>
|_smb-os-discovery:
|   OS: Unix (Samba 3.6.6)
|   Computer name: raspn
|   NetBIOS computer name:
|   Domain name:
|   FQDN: raspn
|_  System time: 2016-09-05T00:15:19+00:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

NSE: Script Post-scanning.
Initiating NSE at 20:19
Completed NSE at 20:19, 0.00s elapsed
Initiating NSE at 20:19
Completed NSE at 20:19, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.17 seconds

```

## APPENDIX D – REVIEW FACTOR GRADING RUBRICS

---

**Table 4** Grading Rubric for Ease of Installation

Grade	Description
1	Installation was not possible or required hardware/software not available during this research.
2	Installation is slow. Documentation is severely limited, and steps required may be convoluted. Beginners may struggle.
3	Install takes time and requires following many steps. Some technical knowledge is required and/or documentation is limited so further research may be necessary.
4	Install is reasonably quick and simple. Requires some technical knowledge and/or documentation is clear but could be easier to understand/more in-depth.
5	Installation is quick and simple. Requires little to no in-depth technical knowledge or is clearly explained in documentation.

**Table 5** Grading Rubric for Documentation

Grade	Description
1	No documentation present. Limited community input.
2	Documentation is lacking. May be limited to install instructions only. Limited community input.
3	Documentation present but only covers the basics.
4	Documentation is available and easy to find. Presented in a reasonable manner but may lack detail in some places.
5	Documentation is available and easy to find. Presented in an easy to digest manner which is suitable for beginners and covers aspects in enough details to support more advanced users too. Active community input/support.

**Table 6** Grading Rubric for Ease of Use

Grade	Description
1	Extremely difficult to use. Beginners would struggle.
2	Steep learning curve to use efficiently. Not particularly intuitive and/or very different to popular operating systems like Windows macOS and even Linux.
3	Reasonable learning curve but not enough to put users off. Similar to popular operating systems but has some key differences.
4	Easy to use. May require some getting used to for beginners but otherwise straightforward with a minimal learning curve.
5	Very easy to use. Minimal learning curve if any. Intuitive for beginners and advanced users alike.

**Table 7** Grading Rubric for Tools Available

Grade	Description
<b>1</b>	Limited number of tools.
<b>2</b>	Limited number of tools but contains a few key tools.
<b>3</b>	Reasonable number of tools. Enough for basic pen testing but may be missing more advanced or popular tools.
<b>4</b>	Good number of tools. Missing only a few major tools.
<b>5</b>	Expansive tool set. Includes nearly all major tools.