ISSN 2278-3091

Volume 10, No.3, May - June 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1031032021.pdf

https://doi.org/10.30534/ijatcse/2021/1041032021

Operating Systems for Ethical Hackers - A Platform Comparison of Kali Linux and Parrot OS

Syed Zain ul Hassan[1], Zainab Muzaffar[2], Saleem Zubair Ahmad[3]
[1,2,3]Department of Software Engineering, Superior University Lahore, Pakistan.
[1]E-mail: zain.ravian@gmail.com, [2]E-mail: zainabmuzaffar228@gmail.com,
[3]E-mail: Saleem.zubair@superior.edu.pk

ABSTRACT

Many operating systems are used for ethical hacking, which has emerged over the years. These operating systems have multiple tools and features to encounter malicious attacks performed by hackers. This study aims to discuss the benefits of various operating systems used for ethical hacking and to present a platform comparison study of two well-known Debian-derived Linux distributions used for ethical hacking, namely Kali Linux and Parrot OS. These tools and features assist ethical hackers in determining which operating system is best for penetration testing. In this paper, we will explore what penetration testing is, why we use this testing technique and how to secure the computer and the network from cyber-attacks using different ethical hacking operating systems. The paper deals with a qualitative analysis of the tools and features to deeply analyze some of their metrics which have been common in these operating systems. This paper will help ethical hackers to nail down the operating systems that are most suitable for them.

Keywords: Operating Systems, Kali Linux, Parrot OS, Penetration testing, Kali vs parrot, Ethical hacking OS, Cyber Security.

1. INTRODUCTION

An operating system is a type of software that has a wide range of definitions and is used to connect human commands to hardware responses [1]. Computers are now considered necessary, from the young to the elderly, from students to business executives. Every year, the number of computer users increases dramatically. The rapid increase in the number of computer users per year raises security concerns. Now, computer security has become critical and attackers are always searching for opportunities and vulnerabilities to gain access to others' personal data.

Penetration testing is a set of activities used to find and exploit security flaws in a computer system [2]. It assists in determining the effectiveness (or ineffectiveness) of the security measures put in place.

Vulnerability assessment's main goal is to find security issues in a controlled environment so that they may be corrected before they are exploited by unauthorized people. Computing system specialists employ penetration testing to resolve issues that appear during vulnerability assessments, with a focus on high-severity defects. Penetration testing is a vital tool for ensuring the security of a system.

Our paper focuses on two well-known Ethical Hacking operating systems that run on machines to perform penetration testing tasks.

We have discussed a platform comparison between Parrot OS and Kali Linux. The comparison of different OSs in terms of their tools and features is needed to provide details on the advantages and disadvantages of both types of OS vis-à-vis their strengths and weaknesses.

1.1 Operating Systems for Ethical Hackers

This research presents different operating systems to be used for Ethical Hacking. Everything is open-source, free, and based on the Linux kernel, with a variety of hacking tools thrown in for good measure. Other Linux distributions are used for ethical hacking, in addition to the Kali distribution and the Parrot OS, which are the most common ones.

1.1.1 Kali Linux [3]

Kali Linux is a widely used open-source security operating system for penetration testing. There are vast array pre-installed penetration testing tools to perform a variety of data security functions, Penetration Testing, Security Analysis, Forensics, and Reverse Engineering are just a few examples.

1.1.2 Parrot OS [4]

Parrot OS is a new version of Linux that comes with several tools for penetration testing. Lightweight with dedicated CDNs. tools such as Anon Surf, Onion Share, TOR, I2P, etc. Parrot Security OS is a hacking distribution that is still in its infancy.

1.1.3 Backbox [5]

The most well-known research techniques are aimed at a broad range of objectives, including web application analysis, network analysis, stress checks, sniffing, vulnerability evaluation, computer forensic analysis, automotive, and exploitation. Backbox is an Ubuntu-based penetration testing and vulnerability assessment distribution. It has its own software repository, which includes the most recent secure versions of many device and network analysis toolkits, as well as the most widely used ethical hacking tools. Backbox is a minimalist desktop environment that runs on the XFCE (XForms Popular Environment). It produces work that is fast, effective, and adaptable.

1.1.4 BlackArch [6]

BlackArch is a comprehensive Linux system for penetration testers and security researchers. It is based on Arch Linux and users can install individual or group BlackArch components directly on top of it. The repository contains 2668 penetration and security tools. Automation, mobile tools & networking.

The toolset is available as an unauthorized Arch Linux user's repository, allowing you to install BlackArch on top of an existing Arch Linux system. Individual packages or categories of packages can be installed.

1.1.5 Fedora Security Lab [7]

Security auditing, forensics, system rescue, and education on security testing methods. Fedora Security Spin is a Fedora version built for security testing and auditing, as well as for educational purposes.

1.1.6 Dracos Linux [8]

Dracos Linux is a penetration testing operating system that is open source. Information collecting, forensics, virus analysis, access management, and reverse engineering are just a few of the pen test tools included. Forensics, information gathering & malware analysis. Having three main directories attack, defense and forensics.

1.1.7 Bugtraq OS [9]

Bugtraq is a software distribution that provides a wide variety of penetration testing, forensic, and laboratory resources. It runs on Ubuntu, Debian, and OpenSUSE and comes with the XFCE, GNOME, and KDE desktop environments. Penetration testing software, mobile forensics, and malware testing facilities, as well as Bugtraq-developed solutions, can all be found on Bugtraq.

1.1.8 CAINE [10]

CAINE Linux is the basis for Pentoo Linux. It's a security and penetration testing delivery that comes as a live CD with persistence. Pentoo uses the XFCE desktop environment, which provides a range of specialized tools and kernel features.

1.1.9 Samurai Web Testing Framework [11]

VMWare supports the Samurai Web Testing Framework as a virtual machine. Perform pen-testing and website attack tools. The Samurai Web Testing Framework was created specifically for web penetration testing. Another distinction from previous distributions is that it is available as a virtual machine, which is compatible with virtual boxes and VMWare. The Samurai Web Testing Platform is a free and open-source framework for testing and targeting websites that is based on Ubuntu.

1.1.10 Network Security Toolkit [12]

It performs regular security checks and network traffic monitoring tasks. Monitoring of virtual machines on a virtual server. The Network Security Toolkit is a Fedora-based bootable Live ISO (Live CD). It includes a large collection of open-source network security software, as well as an integrated web user interface for system and network management, navigation, automation, network control, and analysis, as well as the setup of many of the programs in the distribution.

1.1.11 Demon Linux [13]

Demon Linux is a modified Debian distribution for penetration testing. Hacking tools, VMWare & LIVE with RAM/Squash FS. By pressing just one key, search or open anything.

1.1.12 Arch Strike [14]

Pen testing & security layer, open-source tools for investigation. ArchStrike (previously Arch Assault) is an Arch Linux-based distribution for penetration testers and security professionals. It comes with all of the functionality of Arch Linux, as well as penetration testing and cyber security tools. On the Arch Strike website, tens of thousands of pieces of software and applications are organized into modular kit groups.

1.1.13 Andrax [15]

ANDRAX is a Desktop, Android, and ARM-based Advanced Penetration Testing Platform. Advanced Ethical Hacking and Penetration Testing on Several Platforms performs security checks on a wide range of devices (Desktop, Notebook, Android, Raspberry Pi). ANDRAX makes it possible for devices to be used as a weapon in Advanced Penetration Testing (APT) and Red Team operations.

1.2 A Platform Comparison of Kali Linux and Parrot OS

A platform comparison study of two well-known Debian-derived Linux distributions used for ethical hacking, which are Kali Linux and Parrot OS.

1.2.1 Kali Linux

Kali Linux is an open-source Linux distribution based on Debian that is designed for various information security tasks like penetration testing, security analysis, computer forensics, and reverse engineering [3].Kali Linux is the most effective and widely used penetration testing tool in the world, with penetration testers, forensics experts, reverse engineers, and vulnerability assessors all using it. A large number of tools and utilities are included in the Kali Linux penetration testing platform. Kali Linux enables security and IT experts to examine the security of their systems from data collection to final reporting. Kali Linux comes with a variety of tools that fall into many categories, including [3]:

1.2.1.1 Information Gathering

The act of gathering various types of information against a targeted victim. Table 1 shows 67 different tools used in Kali Linux for gathering information.

Table 1. Information Gathering Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	Ace-voip	24	Amap	47	Nbtscan-unixwiz
2	Automater	25	APT2	48	Bing-ip2hosts
3	CDPSnarf	26	iSMTP	49	copy-router-config
4	Dnmap	27	Dnsenum	50	dnsmap
5	Dnstracer	28	Dnswalk	51	DotDotPwn
6	EnumIAX	29	braa	52	Faraday
7	Firewalk	30	Fragroute	53	fragrouter
8	GoLismero	31	Goofile	54	Cisco-torch
9	InSpy	32	InTrace	55	Metagoofil
10	Maltego Teeth	33	Masscan	56	EyeWitness
11	sslstrip	34	Nikto	57	Ident-user-enum
12	URLCrazy	35	P0f	58	smtp-user-enum
13	SET	36	SMBMap	59	SSLsplit
14	SPARTA	37	Sslcaudit	60	THC-IPV6
15	SSLyze	38	Sublist3r	61	Unicornscan
16	TLSSLed	39	Twofi	62	Xplico
17	Wireshark	40	WOL-E	63	snmp-check
18	Arp-scan	41	Ghost Phisher	64	DNSRecon
19	CaseFile	42	hping3	65	theHarvester
20	DMitry	43	lbd	66	Enum4linux
21	Parsero	44	Miranda	67	OSR Framework
22	Nmap	45	Ntop		
23	Recon-ng	46	Fierce		

1.2.1.2 Vulnerability Analysis

Vulnerability analysis entails discovering, assessing the severity of, and prioritizing any security issues before they are exploited by bad actors. Table 2 shows 27 different tools used in Kali Linux for Vulnerability Analysis.

Table 2. Vulnerability Analysis Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	BBQSQL	10	BED	19	cisco-auditing-tool
2	Cisco-ocs	11	openvas	20	unix-privesc-check
3	SidGuesser	12	sqlsus	21	jSQL Injection
4	Nmap	13	ohrwurm	22	Powerfuzzer
5	HexorBase	14	sfuzz	23	copy-router-config
6	Sqlmap	15	Sqlninja	24	SIPArmyKnife
7	THC-IPV6	16	Yersinia	25	Tnscmd10g
8	Cisco-torch	17	Lynis	26	DotDotPwn
9	Doona	18	Oscanner	27	cisco-global-exploiter

1.2.1.3 Exploitation Tools

Exploitation is a piece of coded software or a script that allows hackers to gain control of a system by exploiting its flaws. Table 3 shows 21 different tools used in Kali Linux for Exploitation Tools.

Table 3. Exploitation Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	Armitage	8	BeEF	15	Backdoor Factory
2	cisco-torch	9	cisco-ocs	16	cisco-auditing-tool
3	crackle	10	exploitdb	17	jboss-autopwn
4	Maltego Teeth	11	MSFPC	18	Metasploit Framework
5	SET	12	ShellNoob	19	RouterSploit
6	Yersinia	13	THC-IPV6	20	Linux Exploit Suggester
7	Commix	14	sqlmap	21	cisco-global-exploiter

1.2.1.4 Wireless Attacks

A harmful activity against wireless system information is referred to as a wireless attack. Table 4 shows 54 different tools used in Kali Linux for Wireless Attacks.

Table 4. Wireless Attacks Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	Airbase-ng	19	Bully	37	Airdecap-ng and Airdecloak-ng
2	airgraph-ng	20	Airmon-ng	38	Airodump-ng
3	Airolib-ng	21	Airserv-ng	39	Airtun-ng
4	Besside-ng	22	Bluelog	40	BlueMaho
5	BlueRanger	23	Bluesnarfer	41	Aircrack-ng

6	crackle	24	Easside-ng	42	eapmd5pass
7	mfoc	25	Ghost Phisher	43	GISKismet
8	gr-scan	26	Spooftooph	44	Packetforge-ng
9	KillerBee	27	Pyrit	45	makeivs-ng
10	mfcuk	28	mfterm	46	FreeRADIUS-WPE
11	mdk3	29	PixieWPS	47	airodump-ng-oui-update
12	redfang	30	RTLSDR Scanner	48	hostapd-wpe
13	Gqrx	31	Wifi Honey	49	wifiphisher
14	Wifite	32	wpaclean	50	Aireplay-ng
15	Kismet	33	coWPAtty	51	kalibrate-rtl
16	Asleap	34	Tkiptun-ng	52	Fern Wifi Cracker
17	Bluepot	35	Wifitap	53	Multimon-NG
18	Reaver	36	ivstools	54	Wesside-ng

1.2.1.5 Forensics Tools

A harmful activity against wireless system information is referred to as a wireless attack. Table 5 shows 23 different tools used in Kali Linux for Wireless Attacks.

Table 5. Forensics Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	Binwalk	9	p0f	17	Capstone
2	Cuckoo	10	dc3dd	18	ddrescue
3	diStorm3	11	Galleta	19	extundelete
4	Xplico	12	peepdf	20	iPhone Backup Analyzer
5	pdf-parser	13	pdfid	21	bulk-extractor
6	RegRipper	14	Volatility	22	Dumpzilla
7	chntpw	15	Foremost	23	Guymager
8	DFF	16	pdgmail		

1.2.1.6 Web Applications

Kali uses the Web applications category to test/penetrate web applications. Table 6 shows 43 different tools used in Kali Linux for Web Applications.

Table 6. Web Applications tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	apache-users	16	Arachni	31	DAVTest
2	Burp Suite	17	CutyCapt	32	fimap
3	DIRB	18	DirBuster	33	hURL
4	Gobuster	19	Grabber	34	Maltego Teeth
5	joomscan	20	jSQL Injection	35	Parsero
6	PadBuster	21	Paros	36	Recon-ng
7	Powerfuzzer	22	ProxyStrike	37	sqlsus
8	sqlmap	23	Sqlninja	38	WebScarab
9	Uniscan	24	w3af	39	Wfuzz
10	WebSlayer	25	WebSploit	40	zaproxy
11	WPScan	26	XSSer	41	Webshag
12	BlindElephant	27	Nikto	42	WhatWeb
13	deblaze	28	plecost	43	jboss-autopwn
14	FunkLoad	29	Skipfish		
15	ua-tester	30	BBQSQL		

1.2.1.7 Stress Testing

Stressing tools are used to stress tests for various applications in order to take suitable preventative steps in the future. Table 7 shows 14 different tools used in Kali Linux for Stress Testing.

Table 7. Stress Testing tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	DHCPig	6	t50	11	FunkLoad
2	inviteflood	7	mdk3	12	ipv6-toolkit
3	rtpflood	8	iaxflood	13	THC-SSL-DOS
4	THC-IPV6	9	Termineter	14	SlowHTTP Test
5	Reaver	10	Inundator		

1.2.1.8 Sniffing & Spoofing

Sniffing and spoofing entails wiretapping the network and monitoring all traffic entering and exiting it. Table 8 shows 33 different tools used in Kali Linux for Sniffing & Spoofing.

Table 8. Sniffing & Spoofing Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	bettercap	12	Burp Suite	23	DNSChef
2	fiked	13	hamster-sidejack	24	HexInject
3	iaxflood	14	inviteflood	25	iSMTP
4	isr-evilgrade	15	mitmproxy	26	ohrwurm
5	protos-sip	16	rebind	27	responder
6	rtpbreak	17	rtpinsertsound	28	rtpmixsound
7	sctpscan	18	SIPArmyKnife	29	SIPp
8	SIPVicious	19	SniffJoke	30	SSLsplit
9	sslstrip	20	THC-IPV6	31	VoIPHopper
10	WebScarab	21	Wifi Honey	32	Wireshark
11	xspy	22	Yersinia	33	zaproxy

1.2.1.9 Password Attacks

When a hacker attempts to steal your password, this is known as a password attack. Table 9 shows 38 different tools used in Kali Linux for Password Attacks.

Table 9. Password Attacks Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	BruteSpray	14	Burp Suite	27	CeWL
2	chntpw	15	cisco-auditing-tool	28	CmosPwd
3	creddump	16	crowbar	29	crunch
4	findmyhash	17	gpp-decrypt	30	hash-identifier
5	Hashcat	18	HexorBase	31	THC-Hydra
6	John the Ripper	19	Johnny	32	keimpx
7	Maltego Teeth	20	Maskprocessor	33	multiforcer
8	Ncrack	21	oclgausscrack	34	ophcrack
9	PACK	22	patator	35	phrasendrescher
10	polenum	23	RainbowCrack	36	rcracki-mt
11	RSMangler	24	SecLists	37	SQLdict
12	Statsprocessor	25	THC-pptp-bruter	38	TrueCrack
13	WebScarab	26	wordlists		zaproxy

1.2.1.10 Maintaining Access

Maintaining Access is a phase of the pentest cycle with a very specific goal: to allow the pentester to stay in the targeted systems until he obtains what he perceives to be important information. Table 10 shows 17 different tools used in Kali Linux for Maintaining Access.

Table 10. Maintaining Access Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	CryptCat	7	Cymothoa	13	dbd
2	dns2tcp	8	HTTPTunnel	14	Intersect
3	Nishang	9	polenum	15	PowerSploit
4	pwnat	10	RidEnum	16	sbd
5	shellter	11	U3-Pwn	17	Webshells
6	Weevely	12	Winexe		

1.2.1.11 Reverse Engineering

The act of deconstructing a thing to see how it works is known as reverse engineering. Table 11 shows 11 different tools used in Kali Linux for Reverse Engineering.

Table 11. Reverse Engineering Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	apktool	5	dex2jar	9	diStorm3
2	edb-debugger	6	jad	10	javasnoop
3	JD-GUI	7	OllyDbg	11	smali
4	Valgrind	8	YARA		

1.2.1.12 Reporting Tools

It's made to make data consolidation, querying, external command execution, and report production simple and straightforward. Table 12 shows 10 different tools used in Kali Linux for Reporting Tools.

Table 12. Reporting Tools [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	CaseFile	5	cherrytree	8	CutyCapt
2	dos2unix	6	Dradis	9	MagicTree
3	Metagoofil	7	Nipper-ng	10	pipal
4	RDPY				

1.2.1.13 Hardware Hacking

Hardware hacking refers to changing an existing piece of electronics to use it in ways it wasn't designed for. Table 13 shows 6 different tools used in Kali Linux for Hardware Hacking Tools.

Table 13. Hardware Hacking [16]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	android-sdk	3	apktool	5	Arduino
2	dex2jar	4	Sakis3G	6	smali

1.2.2 Parrot OS

Parrot is a global group of developers and security experts who collaborate to establish a common framework of tools to make their jobs simpler, more standardized, and safer. Parrot OS, Parrot Security's flagship product, is a Debian-based GNU/Linux distribution built with security and privacy in mind [4]. It includes a complete portable laboratory for all types of cyber security operations, from pen testing to digital forensics and reverse engineering, as well as everything you'll need to write your own software or keep your data secure.

ParrotOS has all of the tools found in Kali Linux, as well as some of its own. Table 8 displays some Parrot OS in-built tools [4].

Table 8. Some Parrot OS in-built tools [3]

Sr.	Tools	Sr.	Tools	Sr.	Tools
1	I2P	8	AnonSurf	15	OnionShare
2	TOR (The Onion Routers)	9	Electrum Bitcoin Wallet	16	Macchanger
3	EtherApe	10	CUPP	17	Ricochet

4	Metasploit Framework	11	Kayak – The Car Hacking Tool	18	GPA – GNU Privacy Assistant
5	Crunch	12	SQLMap	19	Nikto
6	Bleachbit	13	Nmap	20	Aircrack-ng
7	OPENVAS	14	Netcat		

2. LITERATURE REVIEW

In this paper [17], Teddy Surya Gunawan et al. describe that computers and mobile devices connected through the internet exposed to many threats and exploitation [17]. With the help of penetration techniques offered by the Kali Linux operating system, it can be possible to minimize the threat level occurrence thought out the network. The authors explain some of the security parameters present in networks space, implementation of a security breach through penetration technique analysis the security vulnerability and auditing of security through kali Linux tools and techniques. The authors describe in a statically way that the Microsoft Windows OS (83.93% use) and android operating system (69.68% use) are most vulnerable/malicious because of widely used in the world that's why most of the attackers/hackers try to find a vulnerability in it to gain access to the system.

The penetration starts from identifying system vulnerabilities for this purpose the attacks/exploits tools used by authors in his research are (1) SQL Injection tool, (2) cross-site scripting tools, (3) Local/remote file inclusion tool, (4) Distributed Denial of services tool, (5) Man in middle attack tool, (6) Zero-day attack tool. In this paper, we explain more attacks/exploit tools in detail. The authors describe the role of security analysts in vulnerability assessment who collect data during an attack or any attempt of attack are going to perform by hacker, detect flaws in the system and maintain the record of the loopholes in the system through investigation. This investigation helps to find and report vulnerabilities in systems. The parameters of the investigation report include (1) Current situation of attack, (2) Impact of attack, (3) Evolution behavior of attack, (4) Forensic of deployed attack, (5) Prediction Information based on sources. Moreover, the author describes the role of the security audit process, in this process the finding and evaluation of vulnerability are made and the alternatives of this vulnerability are developed. Moreover, the author concludes by defining Kali Linux and the tools using for penetration testing.

The Linux Kernel is responsible for connecting the Android phones' hardware. The Linux Kernel is in charge of a number of assets, including memory, memory storage, memory distribution and de-allocation for the record structure, procedure booking, and system management [18].

3. RESEARCH METHODOLOGY

We conducted an SLR. In our investigation, we compared the platforms Kali Linux and Parrot OS in terms of tools and features. The objective of this research is to recognize a platform comparison of ParrotOS vs Kali Linux (Tools and Features) using an ethical hacking operating system. The study is based on a qualitative approach. The primary resources available include research papers, web blogs, website articles, and newspaper articles on the subject. To get a more detailed and in-depth understanding of this topic, the main goal was divided into the following research questions.

Q1. What are the hardware requirements for installing Kali Linux and Parrot OS?

Q2. Which operating system is best in terms of look and feel (user interface)?

Q3. What kinds of Operating System variants are there for Kali Linux and Parrot OS?

Q4. What kinds of penetration tools do Kali Linux and Parrot OS provides?

Q5. Which OS is better in term of performance comparison?

According to research questions, internet surfing is used to answer the above questions. The main reason for searching the internet is to search out the latest tools and features used by both operating systems.

Here are the highlights of a comparison of Linux distributions based on their hardware requirements, user interface, variations, tools, and performance.

3.1 Hardware Requirements

The minimum processor speed, memory, and disc space necessary to install Windows are among these criteria. Table 9 shows comparisons of both OS in terms of hardware requirements.

Table 9. Comparison in terms of hardware requirements [19].

Kali Linux	**Parrot OS**
Kali Linux is heavy-weight Operating system	Parrot OS is a light-weight operating system.
Kali Linux makes use of a number of tools that require graphical acceleration.	The Parrot OS does not require any graphical acceleration.
A minimum of 1GHZ dual-core CPU is needed.	A minimum of 1GHZ dual-core CPU is needed.
Minimum 2 GB of RAM to install the kali-Linux-default metapackage and the default Xfce4 desktop	Minimum 256MB RAM for i386 and 320MB RAM for AMd64 architectures. 512MB or more is recommended.
Both legacy and UEFI boot modes are supported.	Both legacy and UEFI boot modes are supported.
To install and start working with Kali	To install and start working with Kali Linux, you'll need at

Linux, you'll need at least 20GB of storage space.	least 16GB of storage space.
After installation, Kali Linux has a larger deployment size.	After installation, Parrot OS has a smaller deployment size.
Both 32-bit and 64-bit processors are supported.	The most recent version of Parrot OS only works with 64-bit processors.

3.2 User Interfaces

The operating system provides a user interface (UI), which is an environment in which the user interacts with the machine. Table 10 shows comparisons of both OS in terms of hardware user interface.

Table 10. Comparison in terms of user interfaces [19]

Kali Linux	Parrot OS
Its user interface is based on the Gnome desktop environment.	The Ubuntu-Matte-Desktop-Environment is used.
It has a simpler user interface.	It has much better user interface.
It has hefty specifications and is a little slow.	It's tiny and compact, and it doesn't lag much.

3.3 Variations

The comparison between different variations of both operating systems is shown in Table 11.

Table 11. Comparison in terms of Variations [19]

Kali Linux	Parrot OS
Kali Lite Edition.	Parrot Sec OS Lite Edition.
Kali Full Edition.	Parrot Sec OS Full Edition.
Kali armhf/armel (IoT devices).	Parrot Sec OS Air Edition.
Kali Desktop Variation (e17/KDE/Xfce).	Parrot Sec OS Studio Edition.

3.4 Tools

Table 12 shows a comparison of various tools for both operating systems.

Table 12. Comparison in terms of tools [20]

Kali Linux	Parrot OS
Kali Linux offers a vast array of inbuilt penetration tools.	Parrot OS offers a vast array of inbuilt penetration tools.
It does not come with built-in compilers or IDEs.	It comes with a range of compilers and IDEs pre-installed.
It comes with all of the required hacking tools.	While it contains all of the tools used in Kali, it also adds its own. AnonSurf, Wifiphisher, and Airgeddon are only a few examples.
Support for penetration testing tools only. No dealing with inbuilt tools for development purpose.	A complete development stack that comes pre-installed with the top editors, languages, and tools. Multimedia and office packages are available.

3.5 Performance

Table 13 shows a comparison of the performance of both operating systems.

Table 13. Comparison in terms of performance [21]

Kali Linux	Parrot OS
Kali is a little leggy, and running it on a low-end system can be a nightmare when a brute-force attack is running in the background while you're doing anything else.	It's really light and doesn't lag much, because it can run on low-end systems as well.
Kali Linux has a large user base and a vibrant support community. Large repository.	The Parrot community is rapidly growing and low repository.

4. RESULT AND DISCUSSION

By study different comparison between Kali Linux and Parrot OS. We conclude the followings results:

- Both are helpful when it comes to penetration testing.
- Both are designed according to Debian guidelines.
- Both 32-bit and 64-bit architectures are supported.

When opposed to Kali Linux, ParrotOS wins when it comes to general resources and usable features. ParrotOS includes many of the resources found in Kali Linux, as well as some of its own. There are a few tools on ParrotOS that aren't available on Kali Linux. Let's take a look at a couple of them.

4.1 Wifiphisher [22]

When conducting Wi-Fi security testing, Wifiphisher is one of the tools needed. Clients can be targeted, and attacks can be carried out to easily introduce malware and other malicious software into the victim's network. It's a tool that can be tailored to easily capture and acquire all of the credentials required to penetrate the network in a systematic manner.

4.2 AnonSurf [23]

Anonymity is one of the most important requirements for hacking into anyone's architecture. When working on this, there is no ideal textbook procedure for absolutely being anonymous. Despite the fact that there are several choices, AnonSurf takes the lead because of its powerful ability to use Tor IPtables to anonymize an entire device. Tor is a package that comes preinstalled with Parrot OS and allows you to browse the internet anonymously.

4.3 OnionShare [24]

Onion Transmit is an open source that allows you to securely and anonymously share files of any size through the Tor network. It's extremely safe and simple to use; simply drag and drop your file onto the OnionShare. It will then construct a long random URL that the recipient can use to download the file using the TOR browser over the TOR network.

5. CONCLUSIONS

The goal of this paper is to discuss two Linux-based ethical hacking operating systems, which are Kali Linux and Parrot OS. This paper provides a detailed analysis of their tools and features. Multiple successful tools are integrated into both operating systems, which are specially created to carry out heterogeneous forms of attacks and find vulnerabilities by using penetration testing. Choosing an Operating System for ethical hacking is solely based on user preferences, customization, and system specifications. The purpose of using both operating systems is the same for penetration testing, but they have slightly different audiences. Kali Linux is more focused on security experts who want to use the OS for offensive purposes, whereas Parrot OS is more focused on privacy, anonymity, cryptography, security assessment and software development. Kali is resource intensive. To get the most out of Kali Linux, you should use high-spec hardware. If your hardware resources are limited, choose Parrot OS because it is lightweight and all of the tools run smoothly on low system specifications. In the next research work, we will discuss and compare more Linux variants used for ethical hacking.

REFERENCES

1. Alhassan, H., Bach, C.: **Operating System and Decision Making**. Presented at the April 3 (2014).
2. A. Bacudio, X. Yuan, B. Chu, and M. Jones, **“An Overview of Penetration Testing,”** International Journal of Network Security & Its Applications, vol. 3, pp. 19–38, Nov. 2011, doi: 10.5121/ijnsa.2011.3602.
3. **“Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution,”** Kali Linux. https://www.kali.org/ (accessed May 10, 2021).
4. **“Parrot Security.”** https://www.parrotsec.org/ (accessed Mar. 31, 2021).
5. **“Homepage,”** BackBox.org.https://www.backbox.org/ (accessed May 10, 2021).
6. **“BlackArch Linux - Penetration Testing Distribution.”** https://blackarch.org/ (accessed May 10, 2021).
7. **“SecurityLab.”**https://labs.fedoraproject.org/en/ security/(accessed May 10, 2021).
8. **“Dracos Linux.”** https://dracos-linux.org/ (accessed May 10, 2021).
9. **“Bugtraq – ArchiveOS.”** https://archiveos.org/bugtraq/ (accessed May 10, 2021).
10. “**CAINE Live USB/DVD - computer forensics digital forensics.”** https://www.caine-live.net/ (accessed May 10, 2021).
11. **“Samurai Web Testing Framework – SecTools Top Network Security Tools.”** https://sectools.org/tool/samurai/ (accessed May 10, 2021).
12. **“Network Security Toolkit (NST 32).”** https://www.networksecuritytoolkit.org/nst/index.html (accessed May 10, 2021).
13. **“Demon Linux.”** https://www.demonlinux.com/ (accessed May 10, 2021).
14. **“ArchStrike.”** https://archstrike.org/ (accessed May 10, 2021).
15. **“ANDRAX Hackers Platform.”**https://andrax.thecrackertechnology.com/(accessed May 10, 2021).
16. **“Kali Linux Tools Listing.”** https://tools.kali.org/tools-listing (accessed Jun. 24, 2021).
17. T. Gunawan, M. Lim, N. Zulkurnain, and M. Kartiwi, **“On the Review and Setup of Security Audit using Kali Linux,”** Indonesian Journal of Electrical Engineering and Computer Science, vol. 11, pp. 51–59, Jul. 2018, doi: 10.11591/ijeecs.v11.i1.pp51-59.
18. R. K. R. G, **“Armoring Client and Servers Running on Linux Based Android Platform,”** IJATCSE, vol. 8, no. 3, pp. 479–486, Jun. 2019, doi: 10.30534/ijatcse/2019/22832019.
19. **Parrot OS vs Kali Linux : which is best for Ethical Hacking,** https://ethicalhackersacademy.com/blogs/ethical-hackers-academy/parrot-os-vs-kali-linux
20. **Difference between Kali Linux and Parrot OS**, https://www.geeksforgeeks.org/difference-between-kali-linux-and-parrot-os/, (2020).
21. **“Kali Linux vs Parrot Security OS: Operating System for Penetration Testing in a Nutshell | Hacker Noon.”** https://hackernoon.com/operating-system-for-penetration-testing-in-a-nutshell-kali-linux-vs-parrot-security-os-384809e7b7ae (accessed Jun. 24, 2021). 2021).
22. **“GitHub - wifiphisher/wifiphisher: The Rogue Access Point Framework.”** https://github.com/wifiphisher/wifiphisher (accessed Jun. 21, 2021).
23. **A. Aslam, “Anonsurf – Linux Hint.”** https://linuxhint.com/anonsurf/ (accessed Jun. 21, 2021).
24. **“ OnionShare.”** https://onionshare.org/ (accessed Jun. 24, 2021).