Trustworthiness Assessment of the ParrotOS Hacking Distribution

Executive Summary:

This report provides a comprehensive analysis of the trustworthiness of the ParrotOS hacking distribution project. Through an in-depth examination of the development team, their affiliations, security measures, community feedback, and development practices, the assessment indicates that ParrotOS exhibits characteristics of a trustworthy distribution for cybersecurity professionals and enthusiasts. The core team demonstrates significant expertise in cybersecurity and open-source development. The strong partnership with Hack The Box, a reputable cybersecurity training platform, further enhances its credibility. ParrotOS offers robust mechanisms for verifying the authenticity and integrity of the distribution. While community feedback is largely positive, some concerns regarding stability have been noted. The project has addressed past vulnerabilities with updates and maintains a transparent development process, including a vulnerability disclosure program. Overall, ParrotOS presents itself as a credible and reliable platform for security-related tasks, provided users adhere to recommended security practices.

Analysis of the ParrotOS Development Team:

The Parrot Project is driven by a community of contributors, with a core team leading its development and direction.[1] Key individuals listed on the official ParrotOS team page play crucial roles in various aspects of the project.

Lorenzo Faletra, known as palinuro, serves as the Team Leader, Core Developer, Infrastructure Manager, and Release Manager.[1] His central role underscores his deep involvement in the technical underpinnings of ParrotOS. Information from IMDb indicates that Faletra is a researcher and cybersecurity specialist, as well as a free software militant, dedicated to ethical hacking.[2] He is the founder of Parrot Security CIC, an organization focused on ethical hacking, and his primary work involves researching, developing, and testing tools and techniques for attacking and protecting computer systems.[2] Faletra is also a cybersecurity trainer for HackTheBox and other companies.[2] Kingsland University highlights that Parrot Security OS was created by Lorenzo "Palinuro" Faletra and the Frozenbox team in 2013, with the goal of providing an operating system for penetration testing, vulnerability assessment, computer forensics, and anonymous browsing.[4] His GitHub profile reveals his contributions to Parrot Security and other open-source projects.[5] Interviews with Faletra emphasize his passion for open software, the right to access software, and the

importance of open-source contributions for building a strong curriculum in the IT field.[6] He also discussed the initial creation of ParrotOS as a personal project to meet his specific needs in the cybersecurity sector.[7] This extensive and multifaceted involvement in the project's leadership, core development, and infrastructure management, combined with his professional experience and open-source contributions, strongly suggests a deep understanding of security principles and a firm commitment to the technical integrity of ParrotOS. His leadership and vision are foundational to the project's ongoing development and direction.

Nikos Fountas, with the alias nfou, holds the position of SVP Operations at Hack The Box and serves as a Director and Strategic Advisor at Parrot Sec.[1] His role as SVP Operations at Hack The Box, a well-established platform for cybersecurity training and penetration testing, signifies his expertise in operational management within the cybersecurity domain.[8] Simultaneously, his position as a Director and Strategic Advisor at Parrot Sec indicates his involvement in the strategic decision-making and overall direction of the ParrotOS project.[1] Fountas's professional background includes experience as an International Proposals Manager and a Key Account Manager in the IT sector.[8] He has also obtained a certification in "Introduction to Cyber Attacks" from New York University.[8] Furthermore, he played a role in establishing the HTB University CTF in 2020, demonstrating his engagement with the cybersecurity education community.[15] His contributions to Security Boulevard address challenges in cybersecurity recruiting, reflecting his understanding of the broader industry landscape.[16] The dual roles held by Fountas suggest a significant strategic alignment between ParrotOS and Hack The Box, potentially facilitating resource sharing and mutual benefits. His operational expertise at Hack The Box likely contributes to the organizational structure and strategic planning of the ParrotOS project. His cybersecurity knowledge, supported by his certification and industry insights, adds further credibility to his advisory role within Parrot Security.

Emmanouil Gavriil, known as arkanoid, is the VP Content at Hack The Box and also serves as a Director and Strategic Advisor at Parrot Sec.[1] As VP Content at Hack The Box, he leads initiatives focused on upskilling cybersecurity enthusiasts and professionals through the development of relevant content.[9] Gavriil brings over 20 years of experience in both technical and management roles within the cybersecurity field, having led numerous security projects across various industries.[17] His areas of expertise include security assessments, red and purple teaming, and threat intelligence.[17] His prior experience includes positions such as Director of Cyber Security Operations and Head of Penetration Testing Operations.[18] Gavriil holds a comprehensive set of cybersecurity certifications, including the Offensive Security

Certified Expert (OSCE), eLearnSecurity Mobile Application Penetration Tester (eMAPT), eLearnSecurity Web Application Penetration Tester (eWPT), Offensive Security Wireless Professional (OSWP), and Offensive Security Certified Professional (OSCP).[18] He was also involved with the Greek Cyber Security Team in 2016 [22] and has presented at security conferences.[23] His blog posts on Hack The Box cover topics such as the use of artificial intelligence in cybersecurity and the importance of realistic threat simulation exercises.[17] Gavriil's extensive technical background in penetration testing and security operations, coupled with his leadership in content development at Hack The Box and his advisory role at Parrot Sec, establishes him as a vital connection between the two organizations. His significant experience and numerous industry certifications provide substantial credibility to the security focus of ParrotOS.

Dario Camonita, with the alias danterolle, is listed as a Senior Systems Engineer for ParrotOS.[1] His technical contributions are evident through his GitHub profile, where he is associated with ParrotSec and has developed tools related to Debian and ParrotOS package management.[24] These tools include scripts for repository extraction and parsing, and an API for accessing Debian/ParrotOS package content.[24] His GitLab profile identifies him as a Core Developer and Senior Software Engineer at Parrot Security.[26] Camonita has also been involved in the broader Linux community, as indicated by his participation in Linux Day Catania [27] and his contributions to the Kali Purple project.[28] His GitHub activity shows he follows other cybersecurity-related projects and individuals.[29] Camonita's role as a Senior Systems Engineer, with a focus on package management and system infrastructure, is crucial for the stability, reliability, and maintainability of the ParrotOS distribution. His development of specific tools for managing Debian and ParrotOS packages directly supports the project's core functionality and software delivery processes.

Giulia M. Stabile, known as sh4rk, serves as the Director of Marketing & Operations Manager for ParrotOS.[1] Her IMDb profile indicates an interest in criminology and a desire to specialize in cybersecurity.[30] While her primary role appears to be in the non-technical areas of marketing and operations, her involvement is essential for the project's outreach, community engagement, and overall efficiency. Her TikTok presence offers a glimpse into her broader interests.[31] Stabile was also involved in the partnership announcement between Parrot and Caido, a web security auditing toolkit, highlighting her role in project communications.[33] Although her direct technical cybersecurity experience is less prominent in the provided information, her management of marketing and operations is vital for the sustainability and growth of the ParrotOS project. Her stated interest in cybersecurity suggests an alignment with

the project's mission.

Table 1: ParrotOS Core Team Member Profiles

Name	Nickname	Title/Role	Key Professional Affiliations	Noteworthy Cybersecurity Experience/Certifications
Lorenzo Faletra	palinuro	Team Leader, Core Dev, Infrastructure Manager, Release Manager	Parrot Security CIC, Hack The Box	Cybersecurity researcher, ethical hacker, open software advocate
Nikos Fountas	nfou	SVP Operations, Director & Strategic Advisor	Hack The Box, Parrot Sec	Operational management, strategic advising, Introduction to Cyber Attacks cert.
Emmanouil Gavriil	arkanoid	VP Content, Director & Strategic Advisor	Hack The Box, Parrot Sec	20+ years in security, OSCE, eMAPT, eWPT, OSWP, OSCP
Dario Camonita	danterolle	Senior Systems Engineer	Parrot Security	Systems engineering, Debian/ParrotOS package management
Giulia M. Stabile	sh4rk	Director - Marketing & Operations Manager	Parrot Security	Interest in criminology and cybersecurity

The ParrotOS and Hack The Box Connection:

The relationship between ParrotOS and Hack The Box is significant and multifaceted,

with several key team members holding prominent positions in both organizations.[1] Lorenzo Faletra, the Team Leader of ParrotOS, is also a cybersecurity trainer for Hack The Box and identifies as a Hack The Box employee.[2] Nikos Fountas serves as the SVP Operations at Hack The Box and as a Director and Strategic Advisor for Parrot Sec.[1] Emmanouil Gavriil holds the position of VP Content at Hack The Box while also being a Director and Strategic Advisor at Parrot Sec.[1] This overlap in key personnel strongly suggests a close collaboration and shared vision between the two entities.

Hack The Box actively sponsors the Parrot Security project, indicating a formal commitment to its success.[35] Furthermore, ParrotOS is the chosen operating system for Pwnbox, Hack The Box's innovative in-browser cloud-based virtual hacking distribution.[35] This integration allows Hack The Box users to leverage the extensive tools and features of ParrotOS directly within their web browsers, streamlining the penetration testing and cybersecurity training experience.

In May 2020, Hack The Box and ParrotOS announced a formal partnership with a shared mission to drive innovation within the cybersecurity industry.[39] As part of this collaboration, Hack The Box provides resources and support to the Parrot team, enabling them to focus on further development and the addition of new functionalities to the Parrot Security OS.[40] Parrot OS has also been incorporated into the Hack The Box platform, allowing users to directly experience the distribution and provide valuable feedback to contribute to the project's ongoing success.[40] Even earlier, in 2020, the HTB University CTF featured ParrotOS stickers and t-shirts as prizes, indicating an existing relationship and cross-promotion between the two communities.[15]

The deep connection between ParrotOS and Hack The Box signifies a strong strategic alignment focused on advancing cybersecurity education and providing practical, hands-on training environments. Hack The Box's endorsement and integration of ParrotOS into its platform serve as a substantial validation of the distribution's utility and relevance within the cybersecurity field. The shared involvement of key personnel in leadership and advisory roles within both organizations likely fosters a collaborative ecosystem that mutually benefits both projects, enhancing the credibility and reach of ParrotOS within the cybersecurity community.

Independent Security Audit Assessment:

Information regarding independent security audits conducted specifically on the ParrotOS distribution is limited within the provided research material. However, there is evidence of a third-party security audit focused on a related entity. Bishop Fox, a

recognized offensive-security professional services company, conducted an independent data-privacy and security audit of Parrot's FreeFlight 6 mobile application for the ANAFI series of drones.[41] This audit scrutinized the application's potential security vulnerabilities and privacy issues, ultimately confirming its adherence to Parrot's promise of exceptional data security, protection, and transparency.[42] The scope of the audit included automated vulnerability scanning, source code review, and manual penetration testing on both the iOS and Android versions of the app, as well as its API web services.[42] While this audit provides assurance for the specific FreeFlight 6 application, it does not directly assess the security of the ParrotOS distribution itself.

The research material also mentions that the company, likely Parrot Security CIC given Lorenzo Faletra's address associated with it [3], performs penetration testing at least annually.[43] This indicates an internal commitment to security assessment; however, it does not represent an independent third-party audit of the operating system.

Furthermore, there is a suggestion in the research material about a plan to develop independent security audits for Linux-based security operating systems, including Parrot OS.[44] This indicates an understanding of the value of external validation for such distributions. However, the snippet refers to a planned initiative rather than a completed audit.

Therefore, while a reputable third-party firm (Bishop Fox) has audited a key application associated with Parrot, and the Parrot team conducts internal penetration testing, there is no direct evidence within the provided snippets of a full, independent security audit having been completed on the ParrotOS distribution itself. The planned future audits for security-focused Linux distributions suggest an ongoing awareness of the importance of such assessments for building trust and verifying security.

Methods for Verifying Authenticity and Integrity:

ParrotOS incorporates several robust methods to allow users to verify the authenticity and integrity of the distribution and its software packages. These mechanisms are crucial for ensuring that the downloaded ISO files and updates have not been tampered with and originate from a trusted source.[45]

One primary method involves verifying the checksums of the downloaded ISO files.[45] ParrotOS provides signed lists of cryptographic hashes, including MD5, SHA256, and SHA512, for each of its ISO releases.[45] Users can download the ISO of their choice and then use command-line tools (such as md5sum, sha256sum, or sha512sum in a Linux

terminal) to calculate the hash of their downloaded file.[45] This calculated hash can then be compared against the corresponding hash published on the official ParrotOS website.[45] If the hashes match exactly, it provides a high degree of certainty that the downloaded file is complete and has not been corrupted or maliciously altered.[45] The use of stronger hashing algorithms like SHA256 and SHA512 offers enhanced security against collisions compared to older algorithms like MD5.[48]

In addition to checksum verification, ParrotOS utilizes digital signatures through GPG (GNU Privacy Guard) to ensure the authenticity and integrity of its software repositories and packages.[45] GPG keys are used to digitally sign the repository index files, allowing the apt package manager to verify that the packages being downloaded and installed are indeed from the ParrotOS team and have not been tampered with.[49] ParrotOS provides instructions on how to import the official ParrotOS GPG key, which is essential for this verification process.[45] Recently, Parrot Security updated their GPG keys, which required users to install an updated keyring package to resolve signature verification errors.[49] This proactive management of signing keys is crucial for maintaining a secure update process. The Parrot Mirror Network, which distributes software packages, is also secured by centralized digital signatures, preventing mirrors from injecting fake updates.[51] If a malicious mirror attempts to distribute a tampered package, the Parrot system will automatically refuse to download and install it, raising an alert.[51]

To ensure the integrity of a downloaded ParrotOS ISO, users are advised to first fetch the official ParrotOS GPG key and verify its authenticity.[45] Then, they should download the signed hashes file corresponding to their chosen ISO version from the official website.[45] After downloading the ISO, users should calculate its checksum using the appropriate command-line tool (e.g., sha256sum) and compare the output with the corresponding hash in the signed hashes file.[45] This two-pronged approach, combining checksum verification with GPG key validation for repository integrity, provides a strong assurance of the authenticity and integrity of the ParrotOS distribution.

Cybersecurity Community Perspectives on ParrotOS:

The ParrotOS hacking distribution has garnered significant attention and generated diverse perspectives within the cybersecurity community. Analysis of discussions on online forums, cybersecurity communities like Reddit, and reviews on reputable tech websites reveals a generally positive sentiment towards ParrotOS, alongside some recurring concerns.

Many users and reviewers praise ParrotOS for its user-friendly interface, often noting that it is more intuitive and visually appealing than other security-focused distributions like Kali Linux.[52] Its performance, particularly its lightweight nature and ability to run smoothly on older hardware or in virtual machines, is also frequently highlighted as a key advantage.[52] The extensive collection of pre-installed penetration testing and security tools is another major draw, with some reviewers suggesting that ParrotOS includes even more tools than Kali Linux.[53] The strong focus on privacy and the inclusion of tools like Tor and AnonSurf are also appreciated by users who prioritize online anonymity and security.[53] The availability of a Home Edition, designed for daily use with a focus on privacy and software development, is seen as a significant benefit for those who want a secure operating system for everyday tasks without the full suite of penetration testing tools.[52] The support from and partnership with Hack The Box are viewed positively, indicating a strong connection with a well-regarded platform in the cybersecurity training space.[40]

However, some concerns regarding ParrotOS have been raised within the community. Beginners might find the learning curve steeper compared to more general-purpose Linux distributions due to its specialized tools and focus.[68] Occasional stability issues, particularly after updates or on certain hardware configurations, have been reported by some users.[61] The frequency of updates, while beneficial for security, has also been mentioned as a potential source of instability for some users.[71] Some users perceive the community support for ParrotOS to be less extensive than that of Kali Linux, which has a larger and more established user base.[56] Installation issues and problems with specific hardware configurations have also been reported in some instances.[74] There are also discussions about whether a security-focused distribution like ParrotOS Security Edition is suitable for use as a daily operating system, with some recommending the Home Edition for this purpose while others still advise caution.[66]

Overall, the cybersecurity community generally views ParrotOS favorably as a powerful and versatile distribution for penetration testing, digital forensics, and privacy-focused computing. Its user-friendliness and performance are often cited as advantages over Kali Linux, making it an attractive option for both newcomers and experienced professionals in the field. However, potential users should be aware of the reported stability issues and the learning curve associated with security-centric operating systems.

Past Vulnerabilities and Security Incidents:

Like any complex software system, ParrotOS has experienced its share of vulnerabilities and security incidents. Publicly documented vulnerabilities include

CVE-2023-44451 and CVE-2023-52076, both of which are critical vulnerabilities affecting the Atril document viewer, the default viewer in the MATE desktop environment used by ParrotOS Security Edition.[78] These path traversal and argument injection vulnerabilities could allow remote attackers to achieve remote code execution by writing arbitrary files to the filesystem.[78] It was noted that these vulnerabilities could be particularly impactful against security researchers who often use distributions like Kali and ParrotOS.[78] A patch for CVE-2023-52076 was included in Atril version 1.26.2.[81]

Another significant vulnerability likely affecting ParrotOS is CVE-2023-4911, known as "Looney Tunables".[84] This is a high-severity local privilege escalation vulnerability found in the GNU C Library's dynamic loader due to improper processing of the GLIBC_TUNABLES environment variable.[84] Successful exploitation could allow a local attacker to gain full root privileges on affected Linux systems, including Debian-based distributions like ParrotOS.[84] Patches for this vulnerability were released by major Linux distributions.[86]

A researcher also reported finding zero-day vulnerabilities in multiple popular Linux distributions, including ParrotOS, related to EPUB and CBT file parsing in the default document viewer.[78] These vulnerabilities could lead to remote command execution.[78]

User-reported issues that could have security implications include problems with name resolution ceasing to function after system updates [76] and installation errors related to encrypted partitions, particularly on virtual machines.[74] While not necessarily vulnerabilities in the core OS, these issues can disrupt security workflows and potentially lead to insecure configurations.

ParrotOS maintains a warrant canary, which, as of November 2024, indicated that the project had not been served with any secret government subpoenas.[94] This provides a level of transparency regarding potential legal pressures that could compromise the integrity of the project.

The project appears to be responsive to security issues. The release of patched versions of Atril addresses the identified vulnerabilities in the document viewer.[81] The ParrotOS team also promptly addressed issues with expired GPG keys by providing an updated parrot-archive-keyring package, ensuring the continued secure installation of software.[49] The frequent release of updates, which often include security patches and improvements to core components and security tools, demonstrates an ongoing commitment to addressing vulnerabilities and enhancing the overall security posture

of the distribution.[64]

ParrotOS Development Practices and Transparency:

ParrotOS operates as a community-driven project built upon the Debian Stable branch, following a Long-Term Support (LTS) development model.[1] This foundation provides a stable and well-tested base for the distribution. The project emphasizes transparency by making its source code publicly available on GitLab, with a backup mirror on GitHub.[97] This allows anyone to review, modify, and contribute to the project, fostering community involvement and scrutiny of the codebase.

Contributions from the community are actively encouraged across various aspects of the project, including code development, documentation, and community support.[1] The development workflow typically involves developers writing code, conducting initial local testing, and then involving the broader development team for review and further integration.[107] This collaborative approach helps ensure code quality and identify potential issues early in the development cycle.

ParrotOS offers several editions tailored to different user needs, including Security Edition for penetration testing, Home Edition for daily use with a focus on privacy, Architect Edition for custom installations, and specialized editions for cloud and IoT devices.[38] This variety demonstrates a commitment to catering to a wide range of users within the cybersecurity and privacy-conscious communities.

The ParrotOS project has established a formal vulnerability disclosure program hosted on HackerOne.[111] They encourage security researchers to report any discovered security issues within the current releases of ParrotOS editions, including Security Edition, Home Edition, Docker containers, Raspberry Pi images, and the Hack The Box Edition.[111] The project offers recognition in the form of certificates to researchers who responsibly disclose valid security vulnerabilities.[111] The HackerOne platform facilitates a structured process for reporting, triaging, and addressing security vulnerabilities.

Furthermore, the Parrot Security team frequently releases updates to the operating system and its tools, often highlighting security improvements and the patching of known vulnerabilities in their release notes and blog posts.[64] Security fixes are also provided through the project's software repositories, ensuring that users can easily keep their systems up-to-date with the latest security patches.[51] This proactive approach to vulnerability management and the transparent communication of security updates contribute to the overall trustworthiness of the ParrotOS project.

Overall Reputation and Credibility of ParrotOS:

ParrotOS has cultivated a strong reputation and significant credibility within the cybersecurity community since its initial release in 2013.[38] It is widely recognized as a leading Linux distribution tailored for penetration testing, security auditing, digital forensics, and privacy protection.[4] The distribution has garnered a substantial user base, with over 35 million downloads in the last five years and more than 200,000 unique users.[38]

ParrotOS is frequently compared favorably to Kali Linux, another prominent security-focused distribution. Users and reviewers often cite ParrotOS's user-friendliness, better performance (especially on less powerful hardware), and a broader range of pre-installed tools as advantages.[52] The support from and active partnership with Hack The Box, a highly respected cybersecurity training platform, significantly bolster ParrotOS's reputation and credibility within the professional cybersecurity community.[35] Hack The Box's integration of ParrotOS into its Pwnbox service provides a strong endorsement of the distribution's capabilities and reliability.[35]

The project's longevity, having been active since 2013, and its sustained popularity within the cybersecurity community further contribute to its credibility.[38] The availability of different editions, including a Home Edition designed for general use with a focus on security and privacy, suggests that the project aims to be a versatile operating system beyond just a dedicated penetration testing platform.[38] This broader appeal can enhance trust by indicating a more general-purpose approach to security rather than solely focusing on offensive tools.

Compared to other security-focused distributions, ParrotOS is often positioned as a more user-friendly and resource-efficient alternative to Kali Linux.[52] While BackBox is another Debian-based distribution with a similar focus, ParrotOS appears to have gained more traction and recognition within the community.[52]

Conclusion and Recommendations:

Based on the comprehensive analysis conducted, ParrotOS can be considered a trustworthy distribution for security-related tasks. The development team demonstrates significant expertise in cybersecurity and open-source development. The strong and collaborative partnership with Hack The Box provides further validation of its relevance and utility in the cybersecurity field. ParrotOS offers robust and well-documented methods for users to verify the authenticity and integrity of the

distribution and its software packages, including checksum verification and GPG key validation for its repositories.

While community feedback is largely positive, potential users should be aware of some reported stability issues and the learning curve associated with security-focused operating systems. However, the project has shown responsiveness in addressing past vulnerabilities through updates and patches. The transparent development practices, including the availability of source code and a formal vulnerability disclosure program, contribute to the overall trustworthiness of ParrotOS.

For users considering the adoption of ParrotOS, the following recommendations are provided:

- **Verify the ISO:** Always verify the authenticity and integrity of the downloaded ParrotOS ISO file using the checksum verification and GPG key validation methods outlined in the official documentation.[45]
- **Keep the System Updated:** Regularly update ParrotOS to ensure that you have the latest security patches and bug fixes installed.[64]
- **Be Aware of Potential Issues:** Understand that some users have reported stability issues, so it is advisable to test ParrotOS thoroughly in your specific environment, potentially using a virtual machine, before relying on it for critical tasks.[61]
- **Consider the Home Edition:** If you intend to use ParrotOS for daily tasks in addition to security-related activities, consider using the Home Edition, which is designed for this purpose and has a lighter footprint.[52]
- **Utilize Virtual Machines:** For critical or potentially risky security testing activities, it is recommended to use ParrotOS within a virtual machine to isolate your main system from any potential harm.[118]
- **Engage with the Community:** If you encounter issues or have questions, engage with the active ParrotOS community through their forums and other channels for support and information.[97]
- **Stay Informed:** Keep abreast of any newly disclosed vulnerabilities related to ParrotOS and apply patches promptly to mitigate potential risks.[64]
- **Leverage Security Tools Responsibly:** ParrotOS comes equipped with a wide array of powerful security tools. Ensure that you understand how to use these tools correctly and ethically, and always obtain proper authorization before conducting any penetration testing or vulnerability assessments.[37]

By adhering to these recommendations and staying informed about the project's development and security updates, users can confidently utilize ParrotOS as a

trustworthy platform for their cybersecurity endeavors. The distribution's strong foundation, coupled with its active community and commitment to security, positions it as a valuable asset in the cybersecurity landscape.

Works cited

1. The Team behind ParrotOS, accessed April 8, 2025, https://parrotsec.org/team/
2. Lorenzo Faletra - IMDb, accessed April 8, 2025, https://www.imdb.com/name/nm11366658/
3. Lorenzo Faletra - Palinuro DJ, accessed April 8, 2025, https://palinuro-me-dj.website-eu-central-1.linodeobjects.com/
4. What Are the Best Linux Distros for Cybersecurity Students? - KINGSLAND UNIVERSITY, accessed April 8, 2025, https://kingslanduniversity.com/best-linux-distros-cybersecurity
5. Lorenzo "Palinuro" Faletra PalinuroSec - GitHub, accessed April 8, 2025, https://github.com/palinurosec
6. Hacking, Open Source e Penetration Testing con Palinuro (Lorenzo Faletra) | Tatticata Podcast #15 - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=7zfnJaoZXNs
7. Il mio lavoro? La mia DISTRO | LIVE con Lorenzo Faletra a.k.a. Palinuro @ CommunityVoice - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=To8PJDL1k7M
8. Nikos Fountas - Chief Operating Officer / Company Director & Board Member at Hack The Box | The Org, accessed April 8, 2025, https://theorg.com/org/hack-the-box/org-chart/nikos-fountas
9. Leadership Team - Hack The Box - The Org, accessed April 8, 2025, https://theorg.com/org/hack-the-box/teams/leadership-team-1
10. HRTech Interview with the Director of Operations, Hack The Box, Nikos Fountas, accessed April 8, 2025, https://hrtechcube.com/hrtech-interview-with-nikos-fountas/
11. How Hack The Box Helps Employers Find Brilliant Hackers - HackTheBox, accessed April 8, 2025, https://www.hackthebox.com/blog/connecting-employers-with-hackers
12. Nikos Fountas - Management - Euronet Worldwide, Inc., accessed April 8, 2025, https://ir.euronetworldwide.com/management/nikos-fountas
13. Full text of "Artur Braun EUROMAT 2017" - Internet Archive, accessed April 8, 2025, https://archive.org/stream/FinalEUROMAT2017Web/Final_EUROMAT2017_Web_djvu.txt
14. Team - Parrot Security, accessed April 8, 2025, https://www.parrotsec.org/team/
15. Hack The Box University CTF 2020 Recap, accessed April 8, 2025, https://www.hackthebox.com/blog/htb-uni-2020-recap
16. Nikos Fountas, Author at Security Boulevard, accessed April 8, 2025, https://securityboulevard.com/author/nikos-fountas/
17. Hack The Box blog posts by Emmanouil Gavriil (Arkanoid) - HackTheBox,

accessed April 8, 2025, https://www.hackthebox.com/blog/author/Emmanouil%20Gavriil%20%28Arkanoid%29
18. Emmanouil Gavriil - VP Of Labs At Hack The Box at Hack The Box | The Org, accessed April 8, 2025, https://theorg.com/org/hack-the-box/org-chart/emmanouil-gavriil
19. Your team's next TTX (probably) isn't realistic enough to prep for attacks. Here's why, accessed April 8, 2025, https://www.hackthebox.com/blog/why-the-traditional-ttxs-isnt-realistic-enough
20. Hack The Box blog posts by Noni - HackTheBox, accessed April 8, 2025, https://www.hackthebox.com/blog/author/Noni
21. 30 cybersecurity interview questions and answers (beginner-advanced) - HackTheBox, accessed April 8, 2025, https://www.hackthebox.com/blog/cybersecurity-interview-questions-and-answers
22. The Hellenic Cyber Security Team for ECSC 2016, accessed April 8, 2025, https://ecsc.gr/index.php/en/team-greece-2016-en/
23. T1 07 Detecting and Deceiving the Unknown with Illicium, Andreas Ntakas - Emmanouil Gavriil - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=Zu3TuQs-1bI
24. Dario Camonita danterolle - GitHub, accessed April 8, 2025, https://github.com/danterolle
25. Members · People · ParrotSec - GitHub, accessed April 8, 2025, https://github.com/orgs/ParrotSec/people
26. Dario Camonita - GitLab, accessed April 8, 2025, https://gitlab.com/danterolle
27. Untitled, accessed April 8, 2025, https://www.catania.linux.it/pdf/content/ld2018_locandina.pdf
28. Kali Linux - RSSing.com, accessed April 8, 2025, https://linux1717.rssing.com/chan-10669728/latest.php
29. @Zeref-XXX GitHub Profile - Ÿ HŸPE, accessed April 8, 2025, https://yhype.me/github/@zeref-xxx?tab=followings
30. Giulia Michelle Stabile - IMDb, accessed April 8, 2025, https://www.imdb.com/name/nm11366645/
31. Giulia Stabile (@giugiulol4) oficial - TikTok, accessed April 8, 2025, https://www.tiktok.com/@giugiulol4/?lang=ro-RO
32. Giulia Stabile (@giugiulol4) Official | TikTok, accessed April 8, 2025, https://www.tiktok.com/@MS4wLjABAAAACvzYwygNK0e4VqhCkKsBgKdaN_YGaH4h6oGtpBZA38kVSJGOeJK-dhokDHy86JGv
33. Parrot + Caido, accessed April 8, 2025, https://www.parrotsec.org/blog/2025-01-11-parrot-caido/
34. Lorenzo Palinuro Faletra, accessed April 8, 2025, https://palinuro-me-hack.website-eu-central-1.linodeobjects.com/
35. Installing Parrot Security on a VM | Hack The Box Help Center, accessed April 8, 2025, https://help.hackthebox.com/en/articles/6369713-installing-parrot-security-on-a-

vm
36. Introduction to Pwnbox | Hack The Box Help Center, accessed April 8, 2025, https://help.hackthebox.com/en/articles/5185608-introduction-to-pwnbox
37. Hackers love Pwnbox and its Parrot OS tools. Here's why!, accessed April 8, 2025, https://www.hackthebox.com/blog/pwnbox-parrot
38. Parrot Security, accessed April 8, 2025, https://www.parrotsec.org/
39. Parrot OS + HackTheBox, accessed April 8, 2025, https://parrotsec.org/blog/2020-05-08-parrot-hackthebox/
40. Hack The Box + Parrot OS - HackTheBox, accessed April 8, 2025, https://www.hackthebox.com/blog/supporting-parrot-os
41. Parrot Chooses Bishop Fox for Privacy Audit and Application Penetration Testing, accessed April 8, 2025, https://bishopfox.com/resources/parrot-application-penetration-testing-customer-story
42. Independent Security Audit Confirms Privacy and Security Benefits of Parrot FreeFlight 6 App, accessed April 8, 2025, https://www.parrot.com/en/newsroom/ff6-audit
43. Trust Center - Parrot, accessed April 8, 2025, https://security.parrot.us/controls
44. Setup of the Security Audit Using a Custom Operating System Based, accessed April 8, 2025, https://colab.ws/articles/10.1007%2F978-3-031-71125-1_41
45. Hash and key verification | ParrotOS Documentation - Parrot Security, accessed April 8, 2025, https://parrotsec.org/docs/configuration/hash-and-key-verification/
46. VERIFY MD5 / SHA256 Hash or Checksum on Linux - File Security (Ubuntu) - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=ulln6qVGOJQ
47. What Is Checksum? Guide to Learn Checksum - Simplilearn.com, accessed April 8, 2025, https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-checksum
48. Checksums for Parrot Os : r/linuxmasterrace - Reddit, accessed April 8, 2025, https://www.reddit.com/r/linuxmasterrace/comments/pe2hl3/checksums_for_parrot_os/
49. Parrot rolls out new GPG keys! - Parrot Security, accessed April 8, 2025, https://parrotsec.org/blog/2025-01-11-parrot-gpg-keys/
50. How to resolve 'An error occurred during the signature verification' in Parrot OS after GPG key update?2025 - Stack Overflow, accessed April 8, 2025, https://stackoverflow.com/questions/79352998/how-to-resolve-an-error-occurred-during-the-signature-verification-in-parrot-o
51. Mirrors | ParrotOS Documentation, accessed April 8, 2025, https://parrotsec.org/docs/mirrors/mirrors-list/
52. Parrot Security OS | Review from an openSUSE User - CubicleNate's Techpad, accessed April 8, 2025, https://cubiclenate.com/2019/02/02/parrot-security-os-review-from-an-opensuse-user/
53. Parrot OS Review in the eyes of a Non-Cyber Security Professional | by Arnav Tripathy, accessed April 8, 2025,

https://arnavtripathy98.medium.com/parrot-os-review-in-the-eyes-of-a-non-cyber-security-professional-cf3249397e21
54. Kali Linux vs Parrot OS: Which Pentesting Distro Is Best? - StationX, accessed April 8, 2025, https://www.stationx.net/kali-linux-vs-parrot-os/
55. Why is Parrot OS the best? - Anonymous Hackers, accessed April 8, 2025, https://www.anonymoushackers.net/linux-news/why-is-parrot-os-the-best/
56. Parrot OS Software Reviews, Demo & Pricing - 2025, accessed April 8, 2025, https://www.softwareadvice.com/operating-systems/parrot-os-profile/
57. ParrotOS vs Kali Linux: How to choose the Best - Edureka, accessed April 8, 2025, https://www.edureka.co/blog/parrot-os-vs-kali-linux/
58. Parrot OS v/s Kali Linux : Which is Best for Ethical Hacking | Info-savvy.co, accessed April 8, 2025, https://info-savvy.com/parrot-os-vs-kali-linux-which-is-the-best-for-ethical-hacking/
59. Best forensic and pentesting Linux distro of 2025 | TechRadar, accessed April 8, 2025, https://www.techradar.com/best/best-forensic-and-pentesting-linux-distros
60. Parrot Linux - Review 2023 - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=FspstNpb1Dw
61. Parrot OS Software Reviews, Pros and Cons, accessed April 8, 2025, https://www.softwareadvice.com/operating-systems/parrot-os-profile/reviews/
62. Understanding the Benefits of Using Parrot OS Linux for Penetration Testing | Medium, accessed April 8, 2025, https://medium.com/@techlatest.net/understanding-the-benefits-of-using-parrot-os-linux-for-penetration-testing-28160d5566b
63. Parrot OS 6: The SECRET Weapon Hackers DON'T Want You to Know! (DIGITAL ANARCHY) - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=glQTMeBAMh8
64. Parrot OS 6.2 Release: New Security Tools and Performance Enhancements, accessed April 8, 2025, https://linuxsecurity.com/news/security-projects/parrot-os-6-2-released
65. Best Linux distro's for privacy : r/privacy - Reddit, accessed April 8, 2025, https://www.reddit.com/r/privacy/comments/eje7lf/best_linux_distros_for_privacy/
66. About Parrot OS home edition : r/DistroHopping - Reddit, accessed April 8, 2025, https://www.reddit.com/r/DistroHopping/comments/12tcwby/about_parrot_os_home_edition/
67. Is it advisable to use Parrot OS daily? : r/linuxquestions - Reddit, accessed April 8, 2025, https://www.reddit.com/r/linuxquestions/comments/11szftw/is_it_advisable_to_use_parrot_os_daily/
68. What is ParrotOS?, accessed April 8, 2025, https://parrotsec.org/docs/introduction/what-is-parrot/
69. Solved - Parrot Security | Linux.org, accessed April 8, 2025, https://www.linux.org/threads/parrot-security.44503/
70. Kali vs Parrot vs Athena. The operating system is an integral... | by m5kro |

CyberScribers, accessed April 8, 2025, https://medium.com/cyberscribers-exploring-cybersecurity/kali-vs-parrot-vs-athena-fad387c94f11
71. What are the disadvantages of Parrot OS? - Anonymous Hackers, accessed April 8, 2025, https://www.anonymoushackers.net/linux-news/what-are-the-disadvantages-of-parrot-os/
72. Is it Safe to Main Parrot Security? : r/ParrotOS - Reddit, accessed April 8, 2025, https://www.reddit.com/r/ParrotOS/comments/flnv1m/is_it_safe_to_main_parrot_security/
73. Why most ethical hackers prefer Kali Linux over parrot OS : r/Kalilinux - Reddit, accessed April 8, 2025, https://www.reddit.com/r/Kalilinux/comments/obpyqd/why_most_ethical_hackers_prefer_kali_linux_over/
74. massive issues installing on vmware : r/ParrotSecurity - Reddit, accessed April 8, 2025, https://www.reddit.com/r/ParrotSecurity/comments/1gdpei6/massive_issues_installing_on_vmware/
75. Parrot OS 4.6 - Initial Thoughts - HackerSploit Forum, accessed April 8, 2025, https://forum.hackersploit.org/t/parrot-os-4-6-initial-thoughts/645
76. Parrot OS crazy behavior - Linux.org, accessed April 8, 2025, https://www.linux.org/threads/parrot-os-crazy-behavior.54859/
77. Is making Parrot security as my daily OS good/safe? : r/linuxquestions - Reddit, accessed April 8, 2025, https://www.reddit.com/r/linuxquestions/comments/bi3sso/is_making_parrot_security_as_my_daily_os_goodsafe/
78. I found 2 Zero-Days in popular Linux distros that includes Mint, Kali, Parrot - Febin - Medium, accessed April 8, 2025, https://febinj.medium.com/i-found-2-zero-days-in-popular-linux-distros-that-includes-mint-kali-parrot-04e1cee800bd
79. CVE-2023-44451 - NVD, accessed April 8, 2025, https://nvd.nist.gov/vuln/detail/CVE-2023-44451
80. CVE-2023-44452 - NVD, accessed April 8, 2025, https://nvd.nist.gov/vuln/detail/CVE-2023-44452
81. CVE-2023-52076 Description, Impact and Technical Details - Recorded Future, accessed April 8, 2025, https://www.recordedfuture.com/vulnerability-database/CVE-2023-52076
82. CVE-2023-52076 Detail - NVD, accessed April 8, 2025, https://nvd.nist.gov/vuln/detail/CVE-2023-52076
83. Remote Code Execution Vulnerability in Atril's EPUB ebook parsing - GitHub, accessed April 8, 2025, https://github.com/mate-desktop/atril/security/advisories/GHSA-6mf6-mxpc-jc37
84. CVE-2023-4911: Looney Tunables - Local Privilege Escalation Vulnerability - Picus Security, accessed April 8, 2025, https://www.picussecurity.com/resource/blog/cve-2023-4911-looney-tunables-lo

cal-privilege-escalation-vulnerability
85. Potential Privilege Escalation via CVE-2023-4911 | Elastic Security Solution [8.17], accessed April 8, 2025, https://www.elastic.co/guide/en/security/current/potential-privilege-escalation-via-cve-2023-4911.html
86. HTB enhancing global cybersecurity through collaboration, accessed April 8, 2025, https://www.hackthebox.com/blog/htb-state-partnership-program
87. CVE-2023-4911 Looney Tunables Exploit: Linux GLIBC Vulnerability - Uptycs, accessed April 8, 2025, https://www.uptycs.com/blog/threat-research-report-team/cve-2023-4911-looney-tunables-glibc-exploit
88. Looney Tunables (CVE-2023-4911) exploited for privilege escalation - Datadog Docs, accessed April 8, 2025, https://docs.datadoghq.com/security/default_rules/looney_tunables_exploit/
89. Exploiting the Looney Tunables vulnerability on HTB (CVE-2023-4911), accessed April 8, 2025, https://www.hackthebox.com/blog/exploiting-the-looney-tunables-vulnerability-cve-2023-4911
90. CVE-2023-4911 Detail - NVD, accessed April 8, 2025, https://nvd.nist.gov/vuln/detail/cve-2023-4911
91. Detecting and Mitigating CVE-2023-4911: Local Privilege Escalation Vulnerability | Sysdig, accessed April 8, 2025, https://sysdig.com/blog/cve-2023-4911/
92. CVE-2023-4911: High Severity "Looney Tunables" Vulnerability Impacting Open Source Software | OpenLogic by Perforce, accessed April 8, 2025, https://www.openlogic.com/blog/cve-2023-4911-looney-tunables-centos8-patch
93. CVE-2023-4911: Looney Tunables - Local Privilege Escalation in the glibc's ld.so, accessed April 8, 2025, https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so
94. Warrant Canary - Parrot Security, accessed April 8, 2025, https://www.parrotsec.org/warrant/
95. Parrot 6.1 Release Notes, accessed April 8, 2025, https://parrotsec.org/blog/2024-06-05-parrot-6.1-release-notes/
96. Parrot OS 6.3 Security Advisory: Updates & Tools for Robust Defense, accessed April 8, 2025, https://linuxsecurity.com/news/privacy/parrot-os-6-3-elevating-security-enhanced-features-tools
97. Join the Parrot Community, accessed April 8, 2025, https://parrotsec.org/community/
98. Parrot Security, accessed April 8, 2025, https://parrotsec.org/
99. Parrot OS vs Kali Linux: Which is better? - Simplilearn.com, accessed April 8, 2025, https://www.simplilearn.com/tutorials/cyber-security-tutorial/parrot-os-vs-kali
100. Parrot OS 6 Review: Security-Focused Linux for Privacy - DebugPoint.com, accessed April 8, 2025, https://www.debugpoint.com/parrot-os-6/
101. Parrot OS - Wikipedia, accessed April 8, 2025,

https://en.wikipedia.org/wiki/Parrot_OS
102. Parrot OS Blog, accessed April 8, 2025, https://www.parrotsec.org/blog/
103. parrotsec - GitLab, accessed April 8, 2025, https://gitlab.com/parrotsec
104. Parrot Security · GitHub, accessed April 8, 2025, https://github.com/parrotsec
105. Introduction | ParrotOS Documentation, accessed April 8, 2025, https://parrotsec.org/docs/category/introduction/
106. ParrotOS, what is it and why do you need it? - HackYourMom, accessed April 8, 2025, https://hackyourmom.com/en/osvita/samonavchannya/parrotos-shho-cze-take-i-dlya-chogo-vin-potriben/
107. Community Contributions | ParrotOS Documentation, accessed April 8, 2025, https://parrotsec.org/docs/introduction/community-contributions/
108. Download | ParrotOS Documentation, accessed April 8, 2025, https://parrotsec.org/docs/introduction/download-parrot/
109. Live - Parrot Security, accessed April 8, 2025, https://parrotsec.org/download/
110. ParrotOS: A Comprehensive Guide to the Versatile Security and Development OS | by Raleigh Guevarra | Medium, accessed April 8, 2025, https://medium.com/@raleighguevarra/parrotos-a-comprehensive-guide-to-the-versatile-security-and-development-os-fa209a7c6bf1
111. Parrot Sec | Vulnerability Disclosure Program Policy | HackerOne, accessed April 8, 2025, https://hackerone.com/parrot_sec
112. Parrot Sec | Updates - HackerOne, accessed April 8, 2025, https://hackerone.com/parrot_sec/updates
113. Security-Focused ParrotOS 6.3 Distro Brings New and Updated Tools, Improvements, accessed April 8, 2025, https://9to5linux.com/security-focused-parrotos-6-3-distro-brings-new-and-updated-tools-improvements
114. Parrot 6.3 Release, What's New - GBHackers, accessed April 8, 2025, https://gbhackers.com/parrot-6-3-release/
115. Parrot OS, ParrotOS Linux packaged by Ntegral Inc, optimized cloud-based virtual desktop - Azure Marketplace, accessed April 8, 2025, https://azuremarketplace.microsoft.com/en-us/marketplace/apps/ntegralinc1586961136942.ntg_parrotos_linux?tab=Overview
116. Parrot OS: Powerful Linux Distro for Security and Privacy, accessed April 8, 2025, https://www.tecmint.com/parrot-os-security-linux/
117. Parrot Security OS 6.1 Released - What's New! - GBHackers, accessed April 8, 2025, https://gbhackers.com/parrot-os-6-1/
118. Is Parrot OS safe? - Anonymous Hackers, accessed April 8, 2025, https://www.anonymoushackers.net/linux-news/is-parrot-os-safe/
119. Parrot Security: Penetration Testing Solution from Parrot OS - Evolve Security, accessed April 8, 2025, https://www.evolvesecurity.com/blog-posts/tools-of-trade-parrot-security
120. Penetration Testing and Digital Forensics with ParrotOS | by TechLatest.Net | Medium, accessed April 8, 2025, https://medium.com/@techlatest.net/penetration-testing-and-digital-forensics-w

ith-parrotos-64b4277b0c9a
121. Parrot OS Installation Guide | Setting Up a Secure Virtual Workspace, accessed April 8, 2025, https://www.webasha.com/blog/parrot-os-installation-guide-setting-up-a-secure-virtual-workspace
122. Parrot OS Security edition is a Linux desktop distribution geared for security admins, accessed April 8, 2025, https://www.techrepublic.com/article/parrot-os-security-edition-is-a-linux-desktop-distribution-geared-for-security-admins/
123. Introduction to Pentesting With Parrot - MrW0r57, accessed April 8, 2025, https://mrw0r57.github.io/2020-05-26-introduction-to-pentesting-with-Parrot-OS/
124. Parrot 6.3: What's New in the Latest Ethical Hacking OS? - Chaintech Network, accessed April 8, 2025, https://www.chaintech.network/blog/parrot-6-3-released-enhanced-security-new-tools-virtualization-upgrades-for-cybersecurity-pros/
125. Parrot os - Off-topic - Hack The Box :: Forums, accessed April 8, 2025, https://forum.hackthebox.com/t/parrot-os/634
126. 10 Reasons to prefer Parrot-Sec over Kali Linux : r/hacking - Reddit, accessed April 8, 2025, https://www.reddit.com/r/hacking/comments/8giglw/10_reasons_to_prefer_parrotsec_over_kali_linux/
127. 20 Best Penetration Testing Tools - Security Boulevard, accessed April 8, 2025, https://securityboulevard.com/2022/03/20-best-penetration-testing-tools/
128. Parrot OS - HackTheBox, accessed April 8, 2025, https://www.hackthebox.com/cybersecurity-resources/parrot-os
129. Why I choose Kaisen over Kali and Parrot - Distribution, accessed April 8, 2025, https://forum.kaisenlinux.org/t/why-i-choose-kaisen-over-kali-and-parrot/159
130. Parrot Community, accessed April 8, 2025, https://community.parrotsec.org/
131. Tools | ParrotOS Documentation, accessed April 8, 2025, https://parrotsec.org/docs/category/tools/
132. Reverse Engineering and Reporting with ParrotOS | by TechLatest.Net - Medium, accessed April 8, 2025, https://medium.com/@techlatest.net/reverse-engineering-and-reporting-with-parrotos-8cc7e41afb61
133. Vulnerability and Web Application Analysis with ParrotOS | by TechLatest.Net | Medium, accessed April 8, 2025, https://medium.com/@techlatest.net/vulnerability-and-web-application-analysis-with-parrotos-6695d855e7bd
134. Learn Vulnerability Assessment in Parrot OS Complete Tutorial - Mind Luster, accessed April 8, 2025, https://www.mindluster.com/lesson/195657-video
135. Farial-mahmod/ParrotOS-Vulnerability-Analysis-in-Parrot-Linux - GitHub, accessed April 8, 2025, https://github.com/Farial-mahmod/ParrotOS-Vulnerability-Analysis-in-Parrot-Linu

x
136. 08 - Vulnerability and Web Application Analysis with ParrotOS - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=lEtasj1XEEI
137. Parrot OS Review: The Ultimate Ethical Hacking Distro For Beginners! - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=otT1jKC4wNM