`An Expert Overview of Linux Distributions for Penetration Testing and Ethical Hacking

Linux hacking distributions are specialized operating systems meticulously crafted for cybersecurity professionals, ethical hackers, and security researchers. These distributions come pre-equipped with a vast array of tools and configurations tailored for tasks such as penetration testing, vulnerability analysis, digital forensics, and security research.[1] Their significance in the cybersecurity landscape lies in providing readily available platforms for assessing and bolstering the security of systems and networks. The existence of numerous such distributions underscores a vibrant and diverse community within cybersecurity, each with its own philosophy and approach to offensive security, catering to a wide spectrum of user preferences and skill levels.[1] The user's request for a comprehensive and up-to-date overview, specifically inquiring about Athena OS and Predator OS and having reviewed extensive online resources, highlights the need for expert curation and synthesis of the available information.

A Comprehensive Overview of Linux Hacking Distributions

Linux hacking distributions can be broadly categorized based on their underlying operating system, which often dictates their package management system and general characteristics.

Debian-based Distributions

Debian serves as the foundation for several prominent hacking distributions. **Kali Linux**, developed and maintained by Offensive Security, stands as the most widely recognized distribution in this category.[1] It boasts over 600 pre-installed tools designed for a multitude of security tasks, including information gathering, vulnerability analysis, and wireless attacks.[1] Its extensive documentation and a large, active community contribute significantly to its popularity, making it a valuable resource for both beginners and seasoned professionals.[2] Kali Linux offers versatile installation options, supporting live booting, bare metal installations, virtual machines, containers, mobile platforms, and the Windows Subsystem for Linux (WSL).[2] Its dominance in the field suggests it has become an industry standard, often serving as a natural starting point for individuals entering cybersecurity.[1] However, the sheer volume of tools can initially feel overwhelming to new users.[7]

Parrot Security OS is another Debian-based distribution that has gained considerable traction.[1] It mirrors Kali in some aspects, offering a Security Edition with pre-installed hacking tools, but places a stronger emphasis on privacy and

anonymity.[1] Parrot OS is generally less resource-intensive than Kali and includes additional tools for encryption and online anonymity.[1] It targets a broad audience, including penetration testers, security professionals, journalists, and ethical hackers, and even offers a Home Edition focused on general privacy.[4] Parrot OS presents itself as a strong alternative to Kali, providing similar capabilities with a greater focus on user privacy and potentially better performance on less powerful hardware.[1]

BackBox Linux, based on Ubuntu, distinguishes itself through its simplicity and user-friendliness, making it an appealing choice for beginners.[1] While it may not have as many pre-installed tools as Kali or Parrot, it includes a useful set for web application and network analysis, as well as digital forensics.[1] BackBox provides helpful tips and descriptions for each bundled tool, further aiding novice users.[1] Its design philosophy centers on ease of use, which might be more conducive to learning for individuals new to penetration testing.[1]

DEFT (Digital Evidence and Forensic Toolkit), another Ubuntu-based distribution, is specifically tailored for digital forensics alongside penetration testing.[1] It comes pre-configured with a range of forensic tools designed for evidence acquisition and analysis.[1] DEFT is utilized by various professionals, including military personnel, law enforcement agencies, researchers, and forensic specialists, offering features for file analysis, data recovery, and disk cloning.[1] This highlights the specialized applications of Linux in cybersecurity beyond just offensive tactics.

CAINE (Computer-Aided Investigative Environment), also built on Ubuntu, is primarily focused on digital forensics.[1] It provides numerous tools to assist investigators in recovering, analyzing, and preserving digital data and evidence.[1] A key strength of CAINE is its adherence to forensic best practices, ensuring that evidence collected using this distribution is legally sound.[1] Like DEFT, CAINE underscores the significant role of Linux in the domain of digital forensics.

Network Security Toolkit (NST), based on Fedora, is designed to provide easy access to a collection of open-source network security applications.[11] Its primary focus is on network monitoring and visualization, making it potentially valuable for network analysts and security operations center (SOC) teams.[11]

Other Debian-based distributions mentioned include **Cyborg Hawk** and **Weakerth4n**.[20] Cyborg Hawk was touted for having a large number of tools, including dedicated ones for malware and mobile security analysis, but its lack of recent updates suggests it may not be actively maintained.[13] Weakerth4n focused on wireless cracking tools but also appears to be an older project.[20] Similarly, Ubuntu-based

distributions like **Blackbuntu** and **GnackTrack**, designed for penetration testing and security training, seem to be based on older versions of Ubuntu, indicating they might be outdated.[20] **Tsurugi Linux**, another Ubuntu-based option, focuses on OSINT (Open Source Intelligence), malware analysis, and forensics, targeting threat hunters and analysts.[11]

Arch-based Distributions

Arch Linux, known for its flexibility and rolling release model, serves as the foundation for several powerful hacking distributions. **BlackArch Linux** stands out with its massive repository containing thousands of preconfigured penetration testing tools.[1] While its user interface can be challenging, making it more suitable for advanced users, its extensive toolset is highly valued by experienced researchers and penetration testers.[1] BlackArch is continuously updated with new tools, ensuring users have access to the latest resources.[4] This distribution caters to those who prioritize a vast arsenal of tools over ease of use.[1]

ArchStrike is another Arch-based distribution that provides extra repositories specifically for security research and penetration testing.[1] It is lightweight and can be run directly from a USB drive, offering portability.[1] However, like BlackArch, it is not considered beginner-friendly.[1] ArchStrike offers a more modular approach, allowing users to add security-focused repositories to a base Arch Linux installation, providing flexibility and customization.[1]

Gentoo-based Distributions

Gentoo Linux, a source-based distribution known for its customizability, is the base for **Pentoo**.[1] Pentoo is a minimalist distribution designed for advanced users, allowing them to tailor their penetration testing environment.[1] It integrates seamlessly with existing Gentoo installations and offers comprehensive tools, including network sniffers, vulnerability scanners, and exploitation frameworks.[1] However, its integration with Gentoo means it has a steep learning curve, particularly for beginners.[1] Pentoo is particularly noted for its capabilities in Wi-Fi hacking and hardware-accelerated cracking.[8]

Fedora-based Distributions

Fedora Security Lab is a Fedora-based distribution specifically tailored for security auditing and testing.[1] While it comes with preloaded security tools, it also allows users to configure custom hacking simulators based on their specific testing needs.[1] A notable feature is its version that can be run directly from a USB drive without

requiring installation, providing a portable ethical hacking environment.[1]

Other/Specialized Distributions

Several other distributions cater to specific needs or offer unique approaches. The **Samurai Web Testing Framework (WTF)** is a live Linux environment specifically pre-configured for web penetration testing.[4] It includes a collection of free and open-source hacking tools focused on detecting web vulnerabilities and is often regarded as an optimal operating system for this purpose.[4] Being distributed as a virtual machine enhances its portability and ease of setup.[5]

CommandoVM, developed by the cybersecurity firm Mandiant, is a unique hacking system designed for both new and experienced users with an easy-to-use interface.[5] Its backing by a leading cybersecurity firm suggests a focus on professional-grade tools and a potentially different approach compared to community-driven distributions.

Kali Purple represents an evolution of Kali Linux, focusing on defensive security in addition to penetration testing.[5] It includes over 100 tools specifically for defensive purposes and aims to provide a platform for both red and blue team activities.[16] Kali Purple is still under development, indicating an ongoing expansion of Kali's capabilities.

Distributions like **Alpine** and **Kicksecure** are known for their strong security focus and lightweight nature.[17] While not primarily marketed as hacking distributions with a plethora of pre-installed tools, their security-centric design makes them potential platforms for users to build their own customized penetration testing environments.

Other distributions mentioned in the context of comparisons with Predator OS include **dracOS Linux**, noted for its command-line tools; **Discreete Linux**, regarding boot options and security features; **Kodachi Linux**, for privacy and anonymity features; **Santoku Linux**, specializing in mobile penetration testing; **Whonix**, known for its strong focus on anonymity through Tor; **AttifyOS**, for IoT penetration testing; **stressLinux**, focusing on stress testing; and **IprediaOS**, emphasizing web anonymity.[22] These comparisons highlight the diverse landscape of security-focused Linux distributions, each with its own strengths and target audience.

Spotlight on Athena OS: A Modern Approach to Penetration Testing

Athena OS presents itself as a modern, open-source penetration testing distribution

built upon the foundations of both Arch Linux and Nix/NixOS.[24] It aims to offer a distinct experience compared to traditional distributions by emphasizing reproducibility, flexibility, isolation, and a user-friendly environment despite its Arch and Nix underpinnings.[24]

A key feature of Athena OS is its organized approach to pentesting tools, which are classified by Cyber Roles to enhance efficiency.[24] This categorization helps users quickly find tools relevant to specific security domains. Additionally, the "PWNage" menu provides a convenient, keyboard-centric way to access these tools.[34] Athena OS also focuses on integrating various hacking resources, including direct connections to e-learning platforms like Hack The Box (via HTB Toolkit, HTB Play, and HTB Update), Offensive Security, PWNX, and InfoSec certifications.[24] This integration underscores a commitment to practical learning and engagement with the cybersecurity community.

Performance is another priority for Athena OS, with kernel-level tweaks aimed at improving speed and responsiveness.[24] Its foundation on Arch Linux contributes to this performance, as pacman, Arch's package manager, is known for its speed.[32] Furthermore, Athena OS offers deep customization options through its integration with Nix, allowing users to tailor the environment to their specific needs.[24]

Security is paramount in Athena OS. Leveraging Nix, the distribution focuses on providing secure software by continuously checking packages for known vulnerabilities (CVEs) and preventing the installation of insecure software.[24] All packages developed for Athena are also GPG-signed and maintained in a dedicated public repository, ensuring their integrity.[24]

Athena OS boasts its own repository, which originated as a fork of the BlackArch repository, containing over 2800 pentesting and security tools.[25] Being based on Arch Linux, Athena also benefits from compatibility with the Arch User Repository (AUR), providing access to a vast collection of community-maintained software.[24]

Despite being built on Arch and Nix, which can be perceived as complex, Athena OS strives to provide a user-friendly environment.[24] It offers a choice of multiple shells, including Bash, Fish, Zsh, and PowerShell, with enhancements like autosuggestion and autocompletion to improve the user experience.[32]

Installing Athena OS involves downloading an ISO image and creating a bootable USB drive, similar to other Linux distributions.[35] It is generally recommended to install it within a virtual environment for safe experimentation.[35]

In summary, key features of Athena OS include its organized pentesting tools, deep

integration with hacking resources, performance optimizations, flexibility through Nix, focus on secure software, a vast tool repository inherited from BlackArch, a user-friendly design, and a rolling release model ensuring access to the latest updates.[24] Athena OS represents a modern approach to penetration testing distributions, attempting to bridge the gap between powerful underlying technologies and a streamlined user experience.[29] Its integration with learning platforms like Hack The Box signifies a strong emphasis on practical skill development and community engagement.[24] The choice of Arch and Nix provides access to a massive software ecosystem and advanced system management capabilities.[24]

Spotlight on Predator OS: Emphasizing Security, Privacy, and a Vast Toolset

Predator OS is presented as a security-centric, free, and open-source Linux distribution designed for penetration testing, ethical hacking, privacy, hardening, security, and anonymity.[22] The project emphasizes freedom and community involvement.[22]

The latest versions of Predator OS are based on Debian Stable, utilizing kernel versions 6.6 and 6.1 LTS.[22] It features a fully customized Plasma desktop environment, along with other desktop options like Mate, LXQT, and LXDE, all tailored with specialized menus.[22] Earlier versions were based on Ubuntu.[39]

Predator OS boasts a large collection of pre-installed tools, numbering around 1200 to 1300, organized into over 40 different categories.[22] These tools are sourced from the Debian and Ubuntu repositories, as well as from GitHub.[22]

A unique aspect of Predator OS is its operation in nine distinct security modes: defensive, offensive, privacy, hardened, secured, settings, pretesting, and pen-testing.[22] This allows users to quickly switch to an environment optimized for specific tasks.

Predator OS includes various features aimed at enhancing privacy and security. It incorporates Tor for anonymity, offers hardening against different types of attacks, and includes tools for data destruction.[22] The distribution also mentions disabling access time updates and telemetry collection for improved privacy.[38] Performance is also a consideration, with features included for low latency performance tuning.[22]

Predator OS makes several claims regarding its advantages over other popular distributions. It asserts easier installation and better hardware support compared to Kali, suitability for both beginners and general work compared to Parrot and Kali, and

a lighter download size despite having more tools than BlackArch, Tsurugi Linux, and dracOS Linux.[22] It also claims to include all tools from Parrot, BackBox, and Pentoo Linux, as well as features from distributions like Deft, CAINE, Kodachi, Discreete, Santoku, Whonix, and AttifyOS.[22]

Beyond tools, Predator OS includes a vast collection of resources such as a large password list, lists of red and blue team tools, cloud security tools, cybersecurity roadmaps, security search engines, educational scripts, and training websites.[23]

Installation is facilitated by the Calamares installer, offering an easier and more user-friendly experience.[22] Predator OS supports booting in both live mode and for installation, along with other modes like safe mode, text mode, and forensic mode.[22] Notably, it also claims the ability to run Windows tools on Linux.[23]

Predator OS is developed and maintained by Hossein Seilani, who is also the creator of other Linux distributions like Emperor-OS, Hubuntu, and Little-Psycho.[22]

In essence, Predator OS aims to be a comprehensive and versatile security platform, combining a large toolset with user-friendliness and a strong emphasis on security and privacy.[22] Its unique nine security modes and claims of encompassing features from numerous other distributions position it as an ambitious project in the Linux hacking distribution landscape.[22] The inclusion of a wide array of supplementary resources suggests a holistic approach to cybersecurity education and practice.[23]

Important Note: It is crucial to differentiate between "Predator OS" (the Linux distribution discussed here) and "PREDATOR," which refers to commercial spyware developed by Intellexa. The snippets [46] detail the spyware, which is an entirely separate entity and unrelated to the Linux distribution with the similar name.

Comparative Analysis of Popular Distributions

Choosing the right Linux hacking distribution often involves considering the trade-offs between various factors. **Kali Linux** and **Parrot Security OS**, both based on Debian, offer extensive toolsets but cater to slightly different priorities.[1] Kali Linux, as the industry standard, benefits from vast community support and documentation, making it a strong choice for those entering the field.[2] Parrot OS, while also feature-rich, places a greater emphasis on privacy and may perform better on less powerful hardware.[1]

Contrasting Kali with **BlackArch Linux** reveals a difference in target users.[1] While Kali aims for broader appeal, BlackArch is geared towards experienced researchers and

penetration testers who value its massive repository of tools, even if it comes at the cost of user-friendliness.[1] Parrot OS, with its focus on privacy, offers a different philosophy compared to BlackArch's tool-centric approach.[1]

BackBox stands out for its simplicity, making it a more accessible option for beginners compared to the potentially overwhelming nature of Kali and Parrot.[1] While it may have fewer tools, its user-friendly design can be beneficial for those just starting to learn about penetration testing.[1]

Newer distributions like **Athena OS** are attempting to innovate by focusing on specific aspects. Its integration with learning platforms and its use of Nix for reproducibility and secure package management differentiate it from more traditional distributions. **Predator OS** aims to be a comprehensive solution, claiming to incorporate features from various distributions and introducing the concept of nine distinct security modes.

The choice between these distributions ultimately depends on the user's individual needs, skill level, and priorities.

Choosing the Right Linux Hacking Distribution

Selecting the most suitable Linux hacking distribution requires careful consideration of several factors. The user's experience level with Linux and penetration testing tools is paramount.[1] For individuals new to the field, distributions like BackBox or even Parrot OS (due to its user-friendly Home Edition) might be more approachable than the extensive Kali Linux or the advanced BlackArch.[1] Experienced users, on the other hand, might prefer the vast toolset of BlackArch or the customizability of Pentoo.[1]

The specific security tasks the user intends to perform should also guide their choice. For web application testing, Samurai WTF is specifically designed for this purpose.[4] Those interested in digital forensics might find DEFT or CAINE more suitable due to their pre-installed forensic toolkits.[1] For general penetration testing, Kali Linux and Parrot Security OS remain popular and versatile options.[1]

Hardware limitations can also play a significant role in the choice of distribution. Lighter distributions like Parrot OS or BackBox might perform better on older or less powerful systems compared to resource-intensive options like Kali or BlackArch.[1]

The availability of community support and documentation is another crucial factor, especially for beginners. Kali Linux often excels in this area due to its large and active

user base.[2]

Ultimately, the best way to find the right Linux hacking distribution is to experiment with several options in virtual environments. This allows users to explore different interfaces, tools, and workflows without affecting their primary operating system. Personal preference and comfort level with a particular distribution are often the deciding factors.[12] Regardless of the chosen distribution, a foundational understanding of basic Linux skills is highly beneficial, as most penetration testing tools can be installed on various Linux systems.[12]

Conclusion: The Evolving Landscape of Linux for Ethical Hacking and Penetration Testing

The landscape of Linux distributions for ethical hacking and penetration testing is constantly evolving, with new distributions emerging and existing ones undergoing continuous development.[2] Popular distributions like Kali Linux, Parrot Security OS, BlackArch, and BackBox remain strong contenders, each catering to different user needs and preferences. Newer distributions like Athena OS and Predator OS are introducing innovative features and approaches, focusing on aspects like user-friendliness, integration with learning platforms, specialized security modes, and comprehensive toolsets [based on insights from their respective sections].

Current trends in this domain include a growing emphasis on user experience, making these powerful tools more accessible to a wider audience.[1] There is also a trend towards better integration with online learning platforms and resources, recognizing the importance of continuous skill development in cybersecurity.[24] Specialization for specific security domains, such as web application testing, digital forensics, mobile security, and IoT security, is also becoming more prevalent.[1] Finally, there is an ongoing effort to strike a balance between providing a vast arsenal of tools and maintaining resource efficiency, ensuring these distributions can run effectively on a variety of hardware.[1]

In conclusion, the optimal Linux hacking distribution is not a one-size-fits-all solution. It depends heavily on the individual's experience, the specific tasks they need to perform, their hardware capabilities, and their personal preferences.[12] Continuous learning and adaptation are crucial in the ever-evolving field of cybersecurity, and users are encouraged to explore and experiment with different distributions to find the one that best empowers their security endeavors.

Table 1: Comparison Table of Key Linux Hacking Distributions

Distribution Name	Base OS	Target Audience	Approx. Tools	Default Desktop	Primary Focus/Unique Features	Ease of Use
Kali Linux	Debian	Beginners to Professionals	600+	XFCE/GNOME	Industry standard, extensive documentation, wide tool range	Beginner/Moderate
Parrot Security OS	Debian	Security Professionals, Privacy-focused	800+	XFCE/MATE	Privacy, anonymity, lightweight option	Beginner/Moderate
BackBox	Ubuntu	Beginners	200+	XFCE	Simplicity, user-friendliness, good for learning	Beginner
BlackArch Linux	Arch	Advanced Users	2800+	Openbox/XFCE	Massive tool repository, for experienced penetration testers	Advanced
Pentoo	Gentoo	Advanced Users	400+	Fluxbox/XFCE	Highly customizable, integrates with Gentoo	Advanced
Fedora Security Lab	Fedora	Security Auditing, Education	150+	XFCE	Custom hacking simulators	Moderate

					, live USB option	
Samurai WTF	Linux	Web Penetration Testers	N/A	N/A	Specifically for web application security testing	Moderate
Athena OS	Arch/Nix	InfoSec Professionals, Students	2800+	GNOME	User-friendly Arch/Nix, HTB integration, organized tools	Moderate
Predator OS	Debian	Pen Testers, Privacy-focused	1200+	Plasma	Security modes, large toolset, privacy features	Beginner/ Moderate

Table 2: Athena OS Features Summary

Feature	**Description**	**Snippet ID(s)**
Base System	Arch Linux and Nix/NixOS based	[24]
Core Principles	Reproducibility, flexibility, isolation, user-friendliness	[24]
Tool Organization	Classified by Cyber Roles, "PWNage" menu for easy access	[24]
Hacking Resources Integration	Hack The Box, Offensive Security, PWNX, InfoSec	[24]

	certifications	
Performance	Kernel-level optimizations	24
Customization	Deep customization options using Nix	24
Security Features	Secure software via Nix (CVE checks), GPG-signed packages	24
Repository	Athena repository (fork of BlackArch, 2800+ tools), AUR compatibility	25
User Experience	Aims to reduce complexity of Arch and Nix, multiple shells with enhancements	24

Table 3: Predator OS Features Summary

Feature	Description	Snippet ID(s)
Core Principles	Security, privacy, hardening, anonymity, pen testing, ethical hacking, open-source	22
Base System and Desktop	Debian Stable, customized Plasma (and other options), kernel 6.6 & 6.1 LTS	22
Tool Count and Organization	Around 1200-1300 tools in 40+ categories, sourced from Debian, Ubuntu, GitHub	22
Security Modes	Nine distinct modes for easy access to relevant tools	22
Privacy and Hardening	Tor integration, hardening against attacks, data	22

	destruction, disables telemetry & access time updates	
Performance Tuning	Features for low latency performance	22
Comparison with Other Distros	Claims advantages over Kali, Parrot, BlackArch, etc.	22
Additional Features	Large password lists, red/blue team tools, cloud security tools, training materials, etc.	23
Installation and Boot Options	Easy installation with Calamares, live boot, installation mode, safe mode, etc.	22
Runs Windows Tools	Claimed ability to run Windows tools on Linux	23
Creator	Hossein Seilani (also created Emperor-OS, Hubuntu, Little-Psycho)	22

Works cited

1. 10 Best Linux Operating Systems for Hacking and Pentesting, accessed April 8, 2025, https://online.yu.edu/katz/blog/best-linux-os-for-hacking-pentesting
2. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, accessed April 8, 2025, https://www.kali.org/
3. www.google.com, accessed April 8, 2025, https://www.google.com/search?q=best+hacking+Linux+distributions
4. Top 10 Linux distro for ethical hacking and penetration testing - Infosec, accessed April 8, 2025, https://www.infosecinstitute.com/resources/penetration-testing/top-10-linux-distro-ethical-hacking-penetration-testing/
5. Best OS for Hacking (2025 Ultimate Guide) - StationX, accessed April 8, 2025, https://www.stationx.net/best-os-for-hacking/
6. 14 Best Linux Distros for Ethical Hackers | by Manthan Ghasadiya - Medium, accessed April 8, 2025, https://medium.com/@manthan27ghasadiya/14-best-linux-distros-for-ethical-hackers-20fce1855c01

7. 6 Most Popular Linux Distributions for Ethical Hacking and Pen Testing - CompTIA, accessed April 8, 2025, https://www.comptia.org/blog/linux-distributions-for-ethical-hacking-and-pen-testing
8. 8 Best Linux Distros for Forensics & Pentesting - eSecurity Planet, accessed April 8, 2025, https://www.esecurityplanet.com/products/open-source-distros-for-pentesting-and-forensics/
9. www.google.com, accessed April 8, 2025, https://www.google.com/search?q=penetration+testing+Linux+distros
10. Kali Linux vs Backbox: Pen Testing and Ethical Hacking Linux Distros | UpGuard, accessed April 8, 2025, https://www.upguard.com/blog/kali-linux-vs-backbox-pen-testing-ethical-hacking-linux-distros
11. Top 10 best linux distro for Ethical hacking, penetration testing & cyber security in 2025, accessed April 8, 2025, https://theserverhost.com/blog/post/best-linux-distro-for-ethical-hacking
12. What distro do real pen testers use? : r/cybersecurity - Reddit, accessed April 8, 2025, https://www.reddit.com/r/cybersecurity/comments/skgeu7/what_distro_do_real_pen_testers_use/
13. What OS you use? : r/hacking - Reddit, accessed April 8, 2025, https://www.reddit.com/r/hacking/comments/14d43h0/what_os_you_use/
14. What primary OS do you use for hacking? - Reddit, accessed April 8, 2025, https://www.reddit.com/r/hacking/comments/15hwcqe/what_primary_os_do_you_use_for_hacking/
15. Top Linux Distros for Ethical Hacking and Penetration Testing - SecurityTrails, accessed April 8, 2025, https://securitytrails.com/blog/top-linux-distributions-ethical-hacking-pentesting
16. Best forensic and pentesting Linux distro of 2025 - TechRadar, accessed April 8, 2025, https://www.techradar.com/best/best-forensic-and-pentesting-linux-distros
17. Good Cyber Security Distro for People New to Linux : r/linux4noobs - Reddit, accessed April 8, 2025, https://www.reddit.com/r/linux4noobs/comments/1f633ot/good_cyber_security_distro_for_people_new_to_linux/
18. The Best Hacking OS (Tier List) - YouTube, accessed April 8, 2025, https://m.youtube.com/watch?v=jwJ6e5x0RLg&pp=ygUKI2FIc2JIc3Rvcw%3D%3D
19. A Complete Penetration Testing & Hacking Tools List for Hackers & Security Professionals : r/HowToHack - Reddit, accessed April 8, 2025, https://www.reddit.com/r/HowToHack/comments/ewm1ax/a_complete_penetration_testing_hacking_tools_list/
20. Which are the Preferred Operating Systems of Professional Hackers? - Infosec-Careers.com, accessed April 8, 2025, https://www.infosec-careers.com/which-are-the-preferred-operating-systems-o

f-professional-hackers/
21. BlackArch Linux - Penetration Testing Distribution, accessed April 8, 2025, https://blackarch.org/
22. Penetration testing and Ethical hacking – Penetration testing and Ethical hacking, accessed April 8, 2025, https://predator-os.ir/
23. hosseinseilani/predator-os: The distro is for penetration testing and ethical hacking and also privacy, hardened, secure, anonymized Linux distro.Predator Linux has around 1300 pre-installed tools which are split into 30 several categories. - GitHub, accessed April 8, 2025, https://github.com/hosseinseilani/predator-os
24. Athena OS - GitHub, accessed April 8, 2025, https://github.com/Athena-OS
25. Why Athena OS?, accessed April 8, 2025, https://athenaos.org/en/getting-started/athenaos/
26. Athena OS - DistroWatch.com, accessed April 8, 2025, https://distrowatch.com/athena
27. Repositories - Athena OS, accessed April 8, 2025, https://athenaos.org/en/configuration/repositories/
28. Athena OS | Athena OS, accessed April 8, 2025, https://athenaos.org/
29. Athena OS — Hacking Distribution. Introduction | by S12 - Martian Defense Cybersecurity, accessed April 8, 2025, https://read.martiandefense.llc/athena-os-hacking-distribution-afece181b4dc
30. Athena OS - Dive into a new PentOS : r/hacking - Reddit, accessed April 8, 2025, https://www.reddit.com/r/hacking/comments/vyplrd/athena_os_dive_into_a_new_pentos/
31. Athena OS 2023.02.20 overview | a Arch Linux-based distro focused on Cybersecurity, accessed April 8, 2025, https://www.youtube.com/watch?v=DJ6K_Wv4kFg
32. What is Athena OS and how you can install and configure it? | by Apostolos Chardalias, accessed April 8, 2025, https://apostolos-chardalias.medium.com/what-is-athena-os-and-how-you-can-install-and-configure-it-27dfd699e1c9
33. Athena OS on offsec.tools, accessed April 8, 2025, https://offsec.tools/tool/athena-os
34. Why AthenaOS Could Be Your New Favorite Hacking OS | by Abao Aweikago - Medium, accessed April 8, 2025, https://medium.com/@stage6isd/why-athenaos-could-be-your-new-favorite-hacking-os-00dcb933cece
35. Athena OS: The Ultimate OS for Ethical Hackers? - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=V3yKC7WohHw
36. Pentesting Tools | Athena OS, accessed April 8, 2025, https://athenaos.org/en/resources/pentesting-tools/
37. Shell | Athena OS, accessed April 8, 2025, https://athenaos.org/en/configuration/shell/
38. Predator-os notes, accessed April 8, 2025, https://www.seilany.ir/predator-os/download/post-installation.pdf

39. Predator-OS Introduction, accessed April 8, 2025, https://seilany.ir/predator-os/features/predator-osV2.5-en.pdf
40. Predator-OS: Built for Penetration Testing and Ethical Hacking | Linux Today, accessed April 8, 2025, https://www.linuxtoday.com/blog/predator-os-built-for-penetration-testing-and-ethical-hacking/
41. Predator-OS: A Lightweight Secure Distro for Ethical Hacking and Privacy, accessed April 8, 2025, https://linuxsecurity.com/features/security-spotlight-experience-enhanced-privacy-security-with-predator-os
42. Introducing Predator-OS v3.5 2025 - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=jHnZOkhFKpo
43. Introducing Predator-OS v3.5 Linux - Debian Mailing Lists, accessed April 8, 2025, https://lists.debian.org/debian-publicity/2025/01/msg00025.html
44. Explore Predator-OS 20.04 LTS: A Secure Linux Distro for Pentesters, accessed April 8, 2025, https://linuxsecurity.com/features/what-you-need-to-know-about-the-predator-os-20-04-lts-release
45. Predator-OS Linux - User Guide, accessed April 8, 2025, https://www.seilany.ir/predator-os/download/predator-os-v3-guide-book.pdf
46. Researchers analyzed the PREDATOR spyware and its loader Alien - Security Affairs, accessed April 8, 2025, https://securityaffairs.com/146780/malware/predator-spyware-analysis.html
47. Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware, accessed April 8, 2025, https://blog.talosintelligence.com/mercenary-intellexa-predator/
48. Which distro should I use for learning to hack? : r/linuxquestions - Reddit, accessed April 8, 2025, https://www.reddit.com/r/linuxquestions/comments/1c9urv2/which_distro_should_i_use_for_learning_to_hack/
49. Exploring the Role of Linux in Ethical Hacking - TCM Security, accessed April 8, 2025, https://tcm-sec.com/exploring-the-role-of-linux-in-ethical-hacking/
50. Best Linux Distribution for Hacking - YouTube, accessed April 8, 2025, https://www.youtube.com/watch?v=3gb9NJ45B_I