



Table of Contents X

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

Kali Purple Guide: All You Need to Know

May 10, 2024 Andrew DeVito



**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)

Listen to the article

Kali Purple promises to be your innovative cyber security distribution designed specifically for the defensive side of the cyber realm, offering you a comprehensive toolkit that caters to various aspects of network defense. This newly released platform is based on the NIST Cybersecurity Framework and provides you with a comprehensive suite of tools and features to bolster your security posture.

In this article, we will delve into the unique features and capabilities of Kali Purple, explore the differences between it and the traditional Kali Linux, and examine how it aligns with the NIST Cybersecurity Framework. We will also take a closer look at some of the new tools incorporated into Kali Purple, discuss the concept of SOC-in-a-box architecture, and provide guidance on obtaining and installing the distribution.

Join us as we take a first look at Kali Purple and explore the ins and outs of this impressive platform.

What Is Kali Purple?

Table of Contents

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion

In addition to the Kali Linux ecosystem, creatively tailored for ethical hackers who focus on defensive security strategies. As a Kali Linux platform, Kali Purple seems uniquely positioned to audiences by leveraging the **NIST Cybersecurity Framework**.

NIST Cybersecurity Framework 1.1 comprises five core domains and a risk-based, strategic approach to managing cyber

organization's assets, systems, and data, and understand security risks.

Protect, Implement safeguards to ensure the delivery of critical infrastructure control and data security.

**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)

Identify detection of cyber security events through continuous monitoring and reporting.

Integrate actions upon detecting a cyber security event involving identification, communication, and mitigation.

- **Recover:** Restore services and operations affected by a cyber security event, focusing on recovery planning and continuous improvement.

Unlike traditional Kali Linux, which you may know for its use in offensive security, Kali Purple expands the platform's capabilities by integrating an array of defensive tools and resources designed to equip you with the ability to proactively identify, respond to, and mitigate cyber security threats. This strategic approach should allow Kali Purple to function as a **complementary solution within the Kali Linux family** rather than replacing the existing platform.

Despite being in its early stages of development, Kali Purple has already garnered interest from the cyber security community, with anticipation building around future updates and enhancements that could further refine and expand its feature set and demonstrate clearer use cases. As the platform continues to evolve, Kali Purple could prove to become a valuable resource to help you strengthen your defensive posture.

How Is Kali Purple Different?

Kali Purple distinguishes itself from its Kali Linux counterpart by offering a distinct and tailored approach. Its architecture is designed to support a range of security professionals, from penetration testers to red team operators. The platform's modular nature allows users to select and configure tools based on their specific needs, providing a highly personalized experience.

Table of Contents

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

The primary difference between Kali Purple and traditional Kali Linux is the inclusion of tools specifically curated to bolster defensive security. These tools will be explored in greater detail in subsequent sections, ranging from the predominantly offensive-oriented toolset found in Kali Linux to the new additions in Kali Purple.

Kali Purple runs on the latest Debian kernel, ensuring optimal performance, especially on modern hardware. It also incorporates the most up-to-date software packages to provide a more refined and user-friendly experience.

Level Up in Cyber Security: included with Kali 2023.1:

Join Our Membership Today!

[LEARN MORE](#)

Changes to Thunar file management and panel management. Includes window tiling, widgets, and adding LTS for this version. A major update soon, but some tweaks have been made by Kali Purple. For example, using F4 to open the terminal from the Nautilus file manager.

Another key differentiator is the introduction of the SOC-in-a-box architecture. This innovative design integrates a diverse suite of security operations center (SOC) components into a modular, connected platform, streamlining workflows and facilitating improved collaboration between security professionals.

The intent behind using Kali Purple as a SOC In-A-Box can be described as setting up multiple machines that monitor a network in various ways. Additionally, you could use them to connect as a **red team/blue team** exercise. One thing that seems to point to this is the way the tools are broken out during the installation process. [**More on that later.**](#)

Kali Purple also features **Kali Autopilot**, a powerful attack script-building capability that allows you to automate various tasks and processes, further enhancing the platform's versatility and adaptability.

Kali Purple Hub

Also introduced is Kali Purple Hub, which is designed to allow the community to upload own custom Kali Autopilot scripts.

Table of Contents X

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

- New typing features.

e latest Python release, ensuring compatibility with ols and libraries. The new Python 3.11.2 implements many e version. Here are a few of the changes in this version:

on in tracebacks.

een 10-60%.

odules (tomllib).

s.

Level Up in Cyber Security: [thon Release Notes](#).

Join Our Membership
Today!

[LEARN MORE](#)

ge maintainers work on updating their packages to the latest behavior changes in Python. Namely, **installing older vays function properly**. Kali's recommended method during

this time is to use `apt install python3-<package>`. When 2023.4 comes out towards the end of the year, this may be the only method supported.

By embracing these advancements and strategically expanding its focus to encompass both offensive and defensive security, Kali Purple has demonstrated a commitment to developing a formidable addition to the Kali Linux ecosystem, further solidifying its position as a comprehensive and versatile solution for cyber security professionals.

What New Tools Come With Kali Purple?

Kali Purple introduces a suite of new tools that align with the five domains of the NIST Cybersecurity Framework (CSF) 1.1: *Identify, Protect, Detect, Respond, and Recover*. This alignment ensures that the tools provided cater to a broad range of defensive cyber security tasks, further pointing to Kali Purple's future potential as a comprehensive solution for security professionals.

As a note, we found that many of these newly announced tools weren't available by default in this first release. Instead, many of them needed to be downloaded and installed by following the directions in the Community Wiki. Even more, at the time of writing, a few of the tools have

challenges with regard to executing them on the device. This is perhaps continued evidence that will require regular updates.

Table of Contents X

[What Is Kali Purple?](#)

[How Is Kali Purple Different?](#)

[What New Tools Come With Kali Purple?](#)

[What is SOC In-A-Box](#)

[How Do I Get Kali Purple?](#)

[Conclusion](#)

GVM (Greenbone Vulnerability Management) are crucial in identifying potential vulnerabilities within an organization's infrastructure. By scanning hosts and networks, GVM enables security teams to stay ahead of threats and maintain a strong security posture.

The screenshot shows the Greenbone Security Assistant (GSA) interface running in Mozilla Firefox. The top navigation bar includes links for Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, and Kali Forums. The user is logged in as Admin **admin**. The main dashboard features several cards:

- Level Up in Cyber Security: Join Our Membership Today!**: Includes a "LEARN MORE" button and a large circular graphic.
- CVEs by creation time (Total: 95...)**: A dual-axis line chart showing CVEs per year (solid green line) and total CVEs (dashed green line) from 1990 to 2015. The total CVEs axis ranges from 0 to 16,000, while the CVEs per year axis ranges from 0 to 100,000.
- Hosts topology**: Displays the message "No hosts with topology selected".
- NVTs by Severity Class (Total: 55...)**: A donut chart showing the distribution of NVTs by severity class. The legend indicates:
 - High (Red)
 - Medium (Orange)
 - Low (Blue)
 - Log (Grey)
 Data points: High (2816), Medium (2197), Low (22958), Log (27948).

At the bottom, it says "Backend operation: 0.13s" and "Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net".

[Greenbone Vulnerability Management](#) from the Kali Wiki.

Needs to be installed

Table of Contents

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

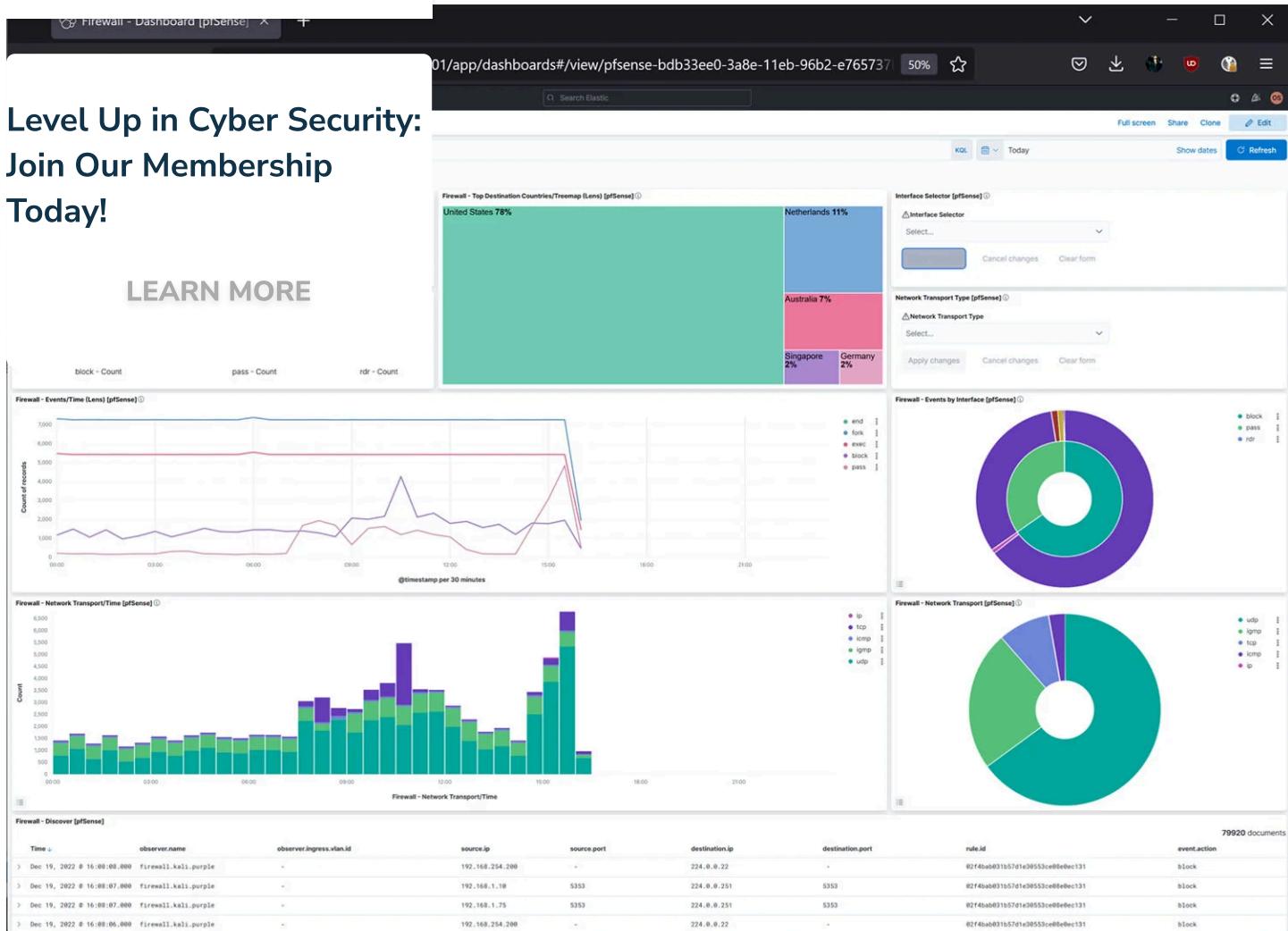
What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

https://gitlab.com/kalilinux/kali-wikis/101_30:-GVM

tools aimed at bolstering an organization's protective **Security**, a powerful Security Information and Event Management (SIEM) system. It consolidates and analyzes security data from various sources, enabling timely detection and mitigation of potential threats. However, it's worth noting that this guide focuses on setting up Elastic Security in Kali Purple.



[Elastic Security](#) from the Kali Wiki.

Needs to be installed

- Installation instructions: https://gitlab.com/kalilinux/kali-wikis/101_40:-Elastic-Agent

Table of Contents

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

own issues with getting all the dependencies installed.

monitoring and analyzing network activity to identify potential threats. Arkime, a network forensics platform, excels in this area, providing deep packet inspection, real-time network traffic monitoring and enabling the early detection of malicious activity. While not a replacement for NetworkMiner, Arkime is a valuable tool that complements NetworkMiner, though it is more complex to use. Overall, Arkime is a powerful tool for network monitoring and analysis, particularly for Kali Purple.

The screenshot shows the Arkime application interface. At the top, there's a navigation bar with links for Home, Files, Stats, History, Settings, and Users. The version is v4.0.2. Below the navigation is a search bar and a date range selector set to 2022/12/22 07:38:55 to 2022/12/22 07:40:00. The main area has tabs for Session, Packets, Bytes, Data bytes, Lines, Bars, and Cap/Restarts. A chart shows network traffic over time. Below the chart is a table with columns for Protocols, Data Source, Log Type, Start Time, Stop Time, Src IP / Country, Src Port, Dst IP / Country, Dst Port, Packets, and Databytes / Bytes. The table lists various network interactions, mostly between 192.168.253.5 and 192.168.253.4, involving protocols like udp, ntp, and icmp.

Protocol	Data Source	Log Type	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes
udp	ntp	zeek	2022/12/22 07:20:33	2022/12/22 07:20:33	192.168.253.5	53065	110.22.64.44 AU	123		
udp	ntp	arkime	2022/12/22 07:20:33	2022/12/22 07:20:33	110.22.64.44 AU	123	192.168.253.5	53065	1	48
udp	ntp	zeek	2022/12/22 07:20:33	2022/12/22 07:20:33	192.168.253.5	53065	110.22.64.44 AU	123	2	96
udp	ntp	zeek	2022/12/22 07:20:33	2022/12/22 07:20:33	192.168.253.5	53065	110.22.64.44 AU	123		152
udp	ntp	arkime	2022/12/22 07:20:33	2022/12/22 07:20:33	192.168.253.5	53065	110.22.64.44 AU	123	1	48
icmp	icmp	zeek	2022/12/22 07:10:13	2022/12/22 07:10:13	fe80::c898:b0ff:fe7c:3 e	133	ff02::2	134	1	0
icmp6	icmp	arkime	2022/12/22 07:10:13	2022/12/22 07:10:13	fe80::c898:b0ff:fe7c:3 e	0	ff02::2	0	1	8
udp	dns	arkime	2022/12/22 06:59:09	2022/12/22 06:59:09	192.168.253.4	53	192.168.253.5	56931	1	95
udp	dns	zeek	2022/12/22 06:59:08	2022/12/22 06:59:08	192.168.253.5	56931	192.168.253.4	53		137
udp	dns	zeek	2022/12/22 06:59:08	2022/12/22 06:59:09	192.168.253.5	56931	192.168.253.4	53	2	135
										191

[Arkime](#) from the Kali Wiki.

Needs to be installed

- Installation instructions: <https://github.com/arkime/arkime>

Overview - Malcolm Dashboard +

Table of Contents

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion

The dashboard includes sections for Log Source, Total Log Count Over Time (bar chart), Application Protocol (table), Actions and Results (table), DNS - Queries (table), and event logs (table). It also features two donut charts for geographical distribution.

**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)

[**Malcolm** from the Kali Wiki.](#)

Needs to be installed

- Installation instructions: https://gitlab.com/kalilinux/kali-purple/documentation/-/wikis/401_20:-Malcolm-Installation

As noted above, there are known issues with getting all the dependencies installed.

Respond

In the event of a security incident, efficient response is crucial. Kali Purple offers **TheHive**, an incident response and forensic tool, to aid security teams in managing and coordinating their response efforts. TheHive provides a collaborative environment where team members can share information, track progress, and streamline the incident response process.

TheHive from The Hive Project.

Severity	Tasks	Observables	Assignee	Date	Actions
Medium	5 Tasks	824		03/20/19 10:56 ① a year	
Medium	5 Tasks	3		02/28/19 14:55 ① a year	
Medium	5 Tasks	53		02/09/17 12:03 ① 3 years	
Low	5 Tasks	5		01/24/17 11:37 ① 4 years	
Low	5 Tasks	10		01/24/17 9:04 ① 4 years	
Low	No Tasks	20		01/22/17 12:17 ① 4 years	

**Level Up in Cyber Security:
Join Our Membership
Today!**

<https://github.com/TheHive-Project/TheHive>

[LEARN MORE](#)

The final domain of the NIST CSF 1.1 involves restoring systems and services to normal operation after a security incident. While Kali Purple does not explicitly introduce tools focused on recovery, the integration of incident response and forensics tools, such as TheHive, can aid you in the development of effective recovery strategies and ensures a swift return to normal operations.

Kali Purple's new tools are intended to provide comprehensive coverage across the five domains of the NIST Cybersecurity Framework, enabling security professionals to effectively identify, protect against, detect, respond to, and recover from cyber threats. With its design to provide a powerful and specialized toolset, Kali Purple aims to enhance how you approach defensive cyber security.

If you want to learn about other tools that come with Kali Purple as part of the core Kali Linux suite, take a look at our article on the [25 Top Penetration Testing Tools for Kali Linux](#).

Table of Contents

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion

Network and System Defense, Security

**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)

Purple Different Than Kali Linux



E

KALI LINUX

Focus

Penetration Testing, Ethical Hacking, Red Teaming

Regular Updates

Latest Kernel

Latest Desktop Environments

Core Kali Linux Tools

Latest Version of Python

Builds on NIST CSF 1.1

- ✓ Identify
- ✓ Protect
- ✓ Detect
- ✓ Respond
- ✓ Recover

Designed for the Five Stages of Ethical Hacking

- ✓ Reconnaissance
- ✓ Scanning
- ✓ Exploitation
- ✓ Maintaining Access
- ✓ Covering Tracks

(As well as other methodologies including the Penetration Testing Execution Standard, MITRE ATT&CK Matrix, etc.)

- ✓ Available as ISO

- ✓ Available as ISO
- ✓ Live Boot Capability
- ✓ Pre-Build VM Images
- ✓ Widely Integrated With AWS, Azure, and Other Cloud-Based Services

Table of Contents X

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion

Kali Autopilot

**Level Up in Cyber Security:
Join Our Membership
Today!**

LEARN MORE

100+ New

600+ Pre-installed Pentesting Tools
Including:

- Metasploit
- Hydra
- Nmap
- SQLMap
- Responder
- Impacket

Extras

- Many Community-Built Tools
- Extensive Documentation



What is SOC In-A-Box



00:00

00:00

1



Kali Purple, addresses this need by offering a streamlined, centralized solution for managing security operations and incident response.

SOC In-A-Box, or Security Operations Center In-A-Box, is an innovative architecture that aims to consolidate essential defensive cyber security tools and processes into a single, cohesive platform. This integrated approach allows you to efficiently monitor, analyze, and respond to threats, vulnerabilities, and incidents in real time.

By bringing together disparate tools and capabilities, SOC In-A-Box empowers you with a unified view of your security posture, thereby enabling you to make informed decisions and take swift, decisive action in response to emerging threats.

Kali Purple's SOC In-A-Box offers you several advantages. It will simplify deployment and configuration, making it easier for you to get up and running with minimal effort. Additionally,

the platform's modular design facilitates the seamless integration of various tools and

Table of Contents X

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

to foster collaboration and information sharing among your team. It's an effective and efficient approach to incident response and threat intelligence management. By reducing reliance on multiple, disparate solutions, streamlining workflows, and reducing the complexity of managing a comprehensive cyber security stack, Kali Purple makes it easier for organizations to stay ahead of emerging threats.

At the moment, getting Kali Purple is a bit of a challenge. You may need to wait for the future development of Kali Purple. However, there are some ways to get started with Kali Purple even if it's not available yet.

Kali Purple?

Getting your hands on Kali Purple is pretty much like getting any other Kali distro. Head over to the official website and download the ISO file.

**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)

There are several ways to get Kali Purple. One option is to download the ISO file from the official website. Another option is to use a virtual machine (VM) to run Kali Purple. There are many pre-built VM images available online, such as Qubes OS, Kali Linux, and Kali Purple. While it's not possible to run Kali Purple directly from a USB drive, it's still possible to do so by using a tool like Kali Live USB.

It's important to note that Kali Purple is not yet available for download. As of now, the only way to get Kali Purple is to wait for its release. However, we believe that the presence of only the ISO file indicates what we've mentioned earlier in this article.



00:00

00:00 1 □



The screenshot shows a video player interface. At the top, there's a navigation bar with a logo, a search bar containing 'Kali Purple', and a 'Table of Contents' section. Below the navigation bar is the main video content area. A red arrow points from the 'Table of Contents' area down towards the video player. The video content itself is a slide from the guide, featuring text about Kali Purple being enterprise grade security accessible to everyone, followed by a large blue button labeled 'Get Started'. In the bottom left corner of the video player, there's a promotional box for 'Kali Purple' membership, which includes a 'LEARN MORE' button and two circular icons labeled '64'.

Let's speed through the installation for an example. While everything else appears exactly like any other Kali or Linux install, our first sense of the changes in Kali Purple occurs on the page where desktop environment selections are made.

KALI

Table of Contents X

[What Is Kali Purple?](#)

[How Is Kali Purple Different?](#)

[What New Tools Come With Kali Purple?](#)

[What is SOC In-A-Box](#)

[How Do I Get Kali Purple?](#)

[Conclusion](#)

installed. The default selections below will install Kali Linux with its standard desktop

environment or a different collection of tools.

[as no effect]

D

[as this item has no effect]

domain IDENTIFY

domain PROTECT

domain DETECT

: domain RESPOND

domain RECOVER

Here you can see the options for the categories of tools that we discussed above. All are security Framework domains. While at first, it may not seem like a

Level Up in Cyber Security: it you could mix and match these tools in various ways.

Join Our Membership Today!

[LEARN MORE](#)

ols for various defense tasks, including network monitoring, response, and forensics, so the possibilities for device configuration

ly Kali hasn't released the VM images yet, and it's unclear if



00:00

00:00 1 □



[Start Hacking Now.](#)

Conclusion

Kali Purple represents a significant leap forward for defensive cyber security, offering a powerful and versatile suite of tools that cater to each of the five domains of the NIST Cybersecurity Framework. By addressing the diverse needs of security professionals, Kali Purple equips you with the means to effectively identify potential threats, implement robust protection measures, detect malicious activity, respond swiftly to security incidents, and recover from cyber attacks.

Kali Purple's holistic approach to cyber security, in combination with its continued commitment to incorporating cutting-edge tools and features, makes it an indispensable asset for security professionals and organizations seeking to bolster their security posture.

As the landscape of cyber security threats continues to evolve, Kali Purple's focus on defensive tools and resources will ensure its relevance. The NIST CSF 1.1 should allow it to remain at the forefront of the tools and resources necessary to navigate the increasingly complex world of cybersecurity.

Table of Contents

What Is Kali Purple?

How Is Kali Purple Different?

What New Tools Come With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

skills yourself, take a look at the below courses available in our



**Level Up in Cyber Security:
Join Our Membership
Today!**

Cybersecurity Boot Camp: Defending Against Hackers

[LEARN MORE](#)

STATIONX

00:00

00:00 1 □



Snort Intrusion Detection, Rule Writing, and PCAP Analysis

4.9 ★★★★★

STATIONX

Table of Contents X

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion



Ethical Hacking: Develop Pentesting Tools

STATIONX

Level Up in Cyber Security:
Join Our Membership
Today!

LEARN MORE

In Cyber Security: Join Our
membership Today!



00:00

00:00 1 □



1≡ Table of Contents X

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion

MEMBERSHIP

Andrew is a Content Writer at StationX. He comes from a multi-discipline professional background with experience in healthcare compliance, financial cyber security

Level Up in Cyber Security: Join Our Membership Today!

[LEARN MORE](#)

Related Articles



00:00



How to Use Ligolo-ng (Easy to Follow Pivoting Tutorial)

[Read More »](#)

00:00 1 □



Top 15+ Cyber Security Tools (2024 Ultimate Guide)

[Read More »](#)

Table of Contents X

- What Is Kali Purple?
- How Is Kali Purple Different?
- What New Tools Come With Kali Purple?
- What is SOC In-A-Box
- How Do I Get Kali Purple?
- Conclusion



Malware Analysis & Exploit Development

OWASP ZAP TUTORIAL



OWASP ZAP Tutorial: Complete 2024 Guide

[Read More »](#)

**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)

SECURITY
ACCESS

CONSULTING

Affiliates



00:00



00:00 1 □

Site Map

Penetration

Incident

Careers

Testing

Response

Media

Vulnerability

Security

Scanning

Architecture

Build Reviews

Risk

Source Code

Assessment

Review

Security

Social

Training

Engineering

Pro Bono

Services

1≡ Table of Contents X

RIGHT © 2024 STATIONX LTD. ALL RIGHTS RESERVED.

What Is Kali Purple?

How Is Kali Purple
Different?

What New Tools Come
With Kali Purple?

What is SOC In-A-Box

How Do I Get Kali Purple?

Conclusion

**Level Up in Cyber Security:
Join Our Membership
Today!**

[LEARN MORE](#)



00:00

00:00

1 □

