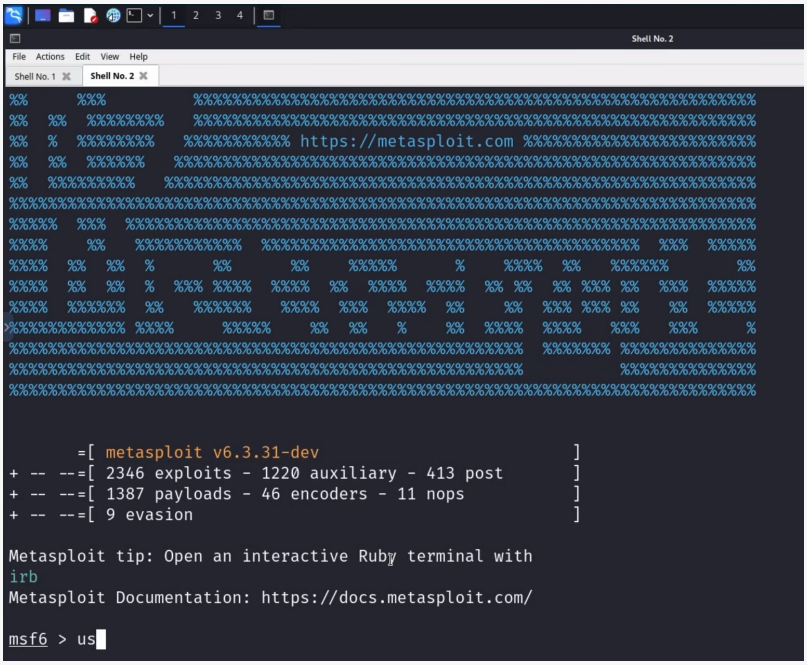
Metasploit Command & Control Featured on Kasm Workspaces

Penetration Testing Command & Control in a Kasm Workspaces for Covert Communication Channel via Reverse Shell over ngrok for Meterpreter Session.

MCLEAN, VA, USA, February 5, 2024 /EINPresswire.com/ -- Kasm Technologies announced a training video demonstrating on-demand pen-testing and vulnerability assessment powered by Metasploit, an open-source phishing framework. These workspaces are detailed in a new video released in cooperation with the Tech Raj YouTube channel.

The video is available at: https://www.youtube.com/watch?v=_9irxRaq9jw
Detailed information is also available on Medium: https://kasm.medium.com/metasploit-command-control-on-kasm-workspaces-80183890a781

Kasm Technologies Logo



Metasploit on Kasm Workspaces

Metasploit is an open-source project for security professionals used to discover and exploit vulnerabilities using the Metasploit Framework (MSF) collection of exploit tools, payloads, and listeners that facilitate the penetration testing process. Metasploit provides users with the resources to perform security assessments, develop and execute exploit code against a remote target machine, and audit systems.

Using Metasploit for Command & Control (C2) purposes allows the attacker to establish a covert communication channel back to the attacking machine through the use of payloads, which can be configured to create a reverse shell or meterpreter session, giving the attacker remote control

over the compromised system. The meterpreter payload is particularly powerful for C2, offering extensive control and interaction capabilities, such as file system manipulation, capturing keystrokes, and webcam control.

Kasm Workspaces, with its containerized approach to delivering browser-based access to desktops, applications, and web services, offers a compelling solution for deploying a Metasploit server in a secure, isolated, and scalable manner. By utilizing Kasm Workspaces, cybersecurity professionals can rapidly spin up instances of Metasploit within Docker containers, ensuring that each session is contained in a secure environment that is segregated from the host system and other workloads. This isolation minimizes the risk of cross-contamination or leakage of sensitive data between sessions, enhancing operational security.

Moreover, Kasm's ability to provide access from any web browser facilitates ease of use and flexibility, allowing users to interact with their Metasploit server from virtually anywhere, without the need for complex VPN setups or direct network access. This approach not only streamlines the process of conducting penetration tests and security assessments but also supports collaboration among security teams by enabling them to access shared tools and resources securely and efficiently.

Since you are using Kali Linux as a docker container you will not be able to receive inbound connections from the internet. However, it is very important for your C&C server to be available on the Internet to receive connections from the targets. To fix this, you can use ngrok to create a secure tunnel from the Internet to your local network interface. This capability allows you to have a C2 server in cloud-hosted Kasm Workspaces instance for your Metasploit cybersecurity pentesting.

For more information on our community edition see: https://www.kasmweb.com/community-edition

ABOUT KASM WORKSPACES
Kasm Workspaces is a container-based platform that offers a flexible and secure environment for remote work and collaboration. With Kasm Workspaces, users can effortlessly create, manage, and deploy containerized desktops and applications, ensuring a seamless and secure user experience. Kasm's core technology revolves around containerized application streaming, which enables users to access a wide array of applications through any web browser, irrespective of their device or operating system. This approach not only enhances accessibility and user experience but also bolsters cybersecurity by isolating each application in a secure container environment.

ABOUT KASM TECHNOLOGIES
Founded by experts in cybersecurity and cloud computing, Kasm Technologies is dedicated to addressing the challenges of modern digital workspaces. Their products are designed to cater to a diverse clientele, ranging from small businesses to large enterprises, offering solutions that

prioritize security, performance, and ease of use. Through its continuous innovation and customer-focused approach, Kasm Technologies is not just redefining the digital workspace but is also contributing significantly to the evolving landscape of cybersecurity and remote work solutions.

Matt
McClaskey
+1 571-444-5276
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube
Other
