

Nessus Vulnerability Scanning Available On-Demand in Kasm Workspaces

Exploiting a Shellshock target on OffSec Proving Grounds Play via ChatGPT crafted inject

MCLEAN, VA, USA, April 18, 2024

/EINPresswire.com/ -- Kasm

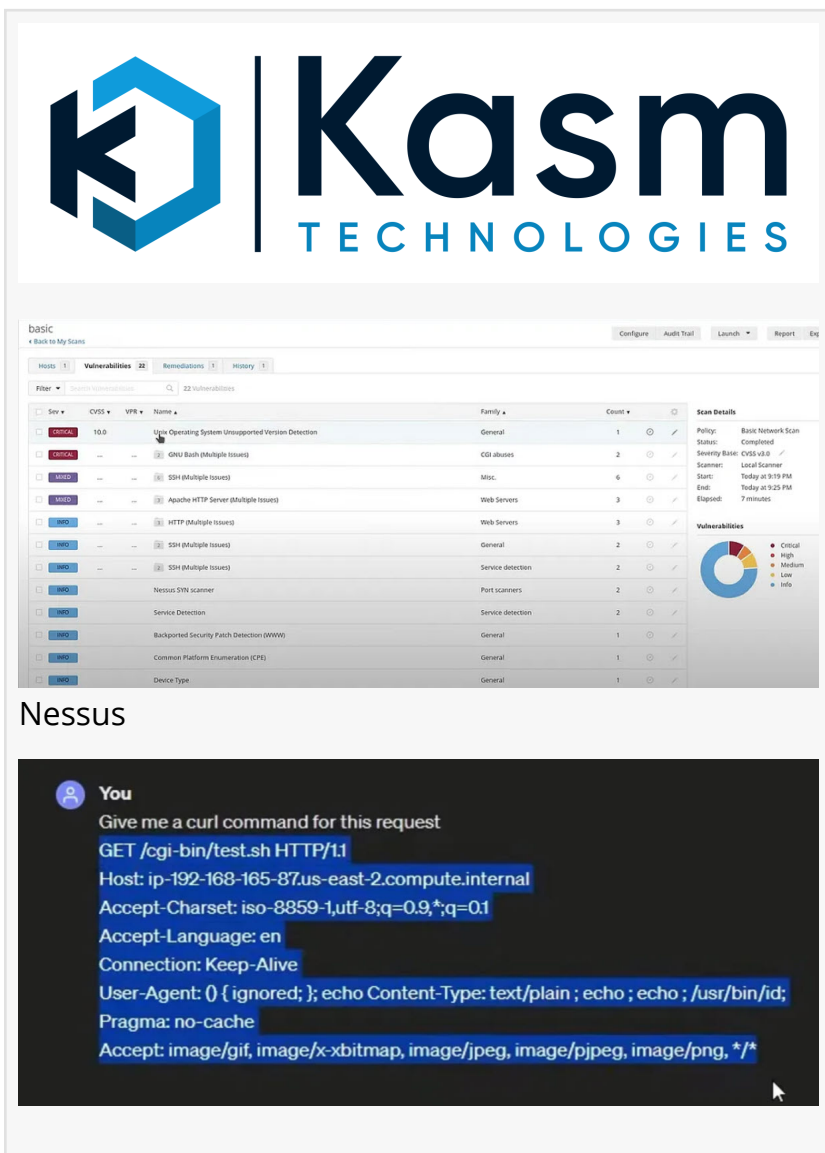
Technologies announced a training video demonstrating on-demand ethical phishing campaigns powered by GoPhish, an open-source phishing framework. These workspaces are detailed in a new video released in cooperation with the Tech Raj YouTube channel.

Kasm Technologies announced a training video demonstrating on-demand vulnerability scanning powered by Nessus. Utilizing Nessus, the industry's most robust vulnerability scanner, alongside the innovative AI capabilities of ChatGPT, this training demonstrates detecting and exploiting the notorious Shellshock vulnerability on the Offsec Proving Grounds Play platform. This workspace is 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=XBt_tsqHoN4

Detailed information is also available on [Medium](#).

Nessus is well-regarded for its comprehensive scanning capabilities that assess entire network attack surfaces to pinpoint vulnerabilities. This tool supports an array of scans, including Host,



The image shows a screenshot of the Kasm Technologies interface. The top part displays the Kasm Technologies logo. Below it, there's a screenshot of the Nessus vulnerability scanner interface. The Nessus interface shows a table of vulnerabilities with columns for Severity, CVSS, VPR, Name, Family, and Count. The table lists various vulnerabilities such as 'Unix Operating System Unsupported Version Detection', 'CGI abuses', 'SSH (Multiple Issues)', and 'Apache HTTP Server (Multiple Issues)'. To the right of the table, there's a 'Scan Details' section showing scan policy, status, severity base, scanner, start and end times, and elapsed time. Below the Nessus screenshot, there's a terminal window showing a curl command for a GET request to a specific host.

Severity	CVSS	VPR	Name	Family	Count
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1
Critical			CGI abuses	CGI abuses	2
High			SSH (Multiple Issues)	Misc.	6
High			Apache HTTP Server (Multiple Issues)	Web Servers	3
High			HTTP (Multiple Issues)	Web Servers	3
High			SSH (Multiple Issues)	General	2
High			SSH (Multiple Issues)	Service detection	2
High			Nessus SSH scanner	Port scanners	2
High			Service Detection	Service detection	2
High			Backported Security Patch Detection (WWW)	General	1
High			Common Platform Enumeration (CPE)	General	1
High			Device Type	General	1

```
You
Give me a curl command for this request
GET /cgi-bin/test.sh HTTP/1.1
Host: ip-192-168-165-87.us-east-2.compute.internal
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: () { ignored; }; echo Content-Type: text/plain ; echo ; echo ; /usr/bin/ld;
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Basic Network, Malware, and Active Directory scans, making it a valuable asset for thorough network enumeration and security breach prevention.

The latest demonstration involved a critical setup of Nessus on Kasm Workspaces, a cutting-edge platform that streams desktops, browsers, and applications directly to the user's web browser. This setup allows Nessus to operate within a container that supports necessary configurations and privileges, thereby enhancing its scanning capabilities.

During this demonstration, Nessus was deployed to scan a designated target machine, aptly named "Sumo," on the Proving Grounds Play network. The scan successfully identified several vulnerabilities, with a particular focus on the "GNU Bash Environment Variable Handling Code Injection (Shellshock)" vulnerability. Nessus not only discovered the vulnerability but also successfully exploited it, confirming the exploit's effectiveness in a live environment.

Further leveraging the AI technology of ChatGPT, Tech Raj utilized the AI to generate a CURL command that replicated the malicious request identified by Nessus. The successful execution of this command by Nessus provided concrete evidence of the vulnerability's presence and the potential for arbitrary command execution on the target system.

Kasm's successful integration of Nessus into our container repo showcases our commitment to support the vulnerability research community. This demonstration emphasizes our ability to equip organizations with the tools necessary to identify and address vulnerabilities promptly, ensuring robust network security in increasingly complex digital landscapes.

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 - CTO

Kasm Technologies

+1 571-444-5276

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/704791048>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.